Juridische aspecten van het gebruik van webcrawlers in de handhaving en opsporing

Lodder, A.R.; Borgers, M.J.; Neerhof, A.R.

2015

Juridische aspecten van het gebruik van webcrawlers in de handhaving en opsporing

A.R. Lodder
M.J. Borgers
A.R. Neerhof

Over de auteurs

Prof. mr. A.R. Lodder

Arno R. Lodder (1967) is hoogleraar Internet Governance and Regulation aan de Vrije Universiteit Amsterdam en hoofd van de afdeling Transnational Legal Studies. Sinds 2014 is hij tevens verbonden aan SOLV advocaten als Of Counsel. In zijn onderzoek en onderwijs richt hij zich op onderwerpen op het snijvlak van recht en internet, zoals aansprakelijkheid, contracteren, security, privacy, vrijheid van meningsuiting, cybercrime alsmede verschijnselen als big data, web 2.0, virtuele werelden, cyberwar, het internet van dingen en smartphones en apps. Hij schreef en redigeerde meer dan 25 boeken, zoals, e-Directives, Guide To European Union Law On E-commerce (2002), Information Technology and Lawyers. Advanced Technology in the Legal Domain (2006), Enhanced Dispute Resolution Through the Use of Information Technology (2010) en Recht en Computer (2014). Tevens schreef hij het voor een groter publiek bedoelde Over de grenzen van het internet, 45 verhalen over recht en onrecht op Facebook, Youtube, Marktplaats, Twitter, Pirate Bay en andere plekken (2014).

Prof. mr. M.J. Borgers

Matthias Borgers (1973) is na afronding van zijn rechtenstudie aan de Universiteit Maastricht in 1996 als onderzoeker-in-opleiding gaan werken bij de Katholieke Universiteit Brabant (nu: Universiteit van Tilburg). In 2001 is hij daar cum laude gepromoveerd op een proefschrift over de ontnemingsmaatregel. Nadien is hij werkzaam geweest als advocaat bij het kantoor van de landsadvocaat (Pels Rijcken & Droogleever Fortuijn, Den Haag) en als universitair (hoofd)docent aan de Universiteit van Tilburg. Sinds 1 maart 2006 is als hoogleraar straf(proces)recht verbonden aan de Vrije Universiteit Amsterdam. In de periode 2008-2011 was hij, als portefeuillehouder onderzoek, lid van het faculteitsbestuur. Thans is hij voorzitter van de afdeling Strafrecht & Criminologie. Het lopende onderzoek van Matthias Borgers concentreert zich rondom het strafprocesrecht. Voorts besteedt hij met enige regelmaat aandacht aan het Europees strafrecht en de rol van het strafrecht bij terrorismebestrijding. Ook de rechtsvinding in het strafrecht, in het bijzonder de rol van het legaliteitsbeginsel, heeft zijn belangstelling.

Dr. A.R. Neerhof

Richard Neerhof (1964) is sinds 1 augustus 2008 werkzaam bij de afdeling Staats- en bestuursrecht. Richard studeerde in 1989 af in de Juridische Bestuurswetenschappen aan de Rijksuniversiteit Groningen. Hij promoveerde in 1995 aan dezelfde universiteit op een proefschrift over rechtsvorming door de bestuursrechter: ‘Het geschil voorbij. Een studie naar de bruikbaarheid van bestuursrechtelijke jurisprudentie als kenbron van recht.’ Hij was eerder werkzaam aan de universiteiten van Utrecht, Maastricht en Groningen, waar hij zich aanvankelijk richtte op het gebied van het algemeen bestuursrecht. Vanaf 1999 specialiseerde hij zich ook in het overheidsaansprakelijkheidsrecht en het omgevingsrecht. Richard is van 2004 tot 2006 werkzaam geweest in de juridische adviespraktijk. Richard verricht onderzoek in het programma in het onderzoeksprogramma “Public Contracts: Law & Governance’. Aan dit onderzoeksprogramma nemen medewerkers van de afdelingen staats- en bestuursrecht en privaatrecht deel. Kern van zijn onderzoeksactiviteiten betreft vraagstukken van regulering en rechtshandhaving en de verdeling van verantwoordelijkheden en risico’s tussen overheid en private partijen daarbij. Daarbij gaat de aandacht in het bijzonder uit naar normstelling en toezicht door private instellingen met het oog op publieke belangen en de relatie hiervan tot wetgeving en besluitvorming door bestuursorganen.

Voorwoord

De automatisering binnen de politie kent een roerige geschiedenis. In de tijd dat er 25 autonoom opererende politiekorpsen waren, was er ongeveer per korps andere software in gebruik. Geautomatiseerde uitwisseling van informatie met het Openbaar Ministerie was mede om die reden lange tijd zo niet onmogelijk toch zeker bijzonder lastig. De hoop en verwachting is dat door de reorganisatie van 1 januari 2013 onder meer inhoudende de vorming van één politiekorps voor heel Nederland de ICT huishouding binnen de politie beter afgestemd en uniformer zal worden. Dit rapport gaat over een specifieke, voor de politie in ontwikkeling zijnde ICT toepassing: Web Voyager. Deze zogenaamde webcrawler vergaart geautomatiseerd op internet aanwezige informatie. In dit onderzoek wordt ingegaan op de vraag of het bestuursrecht (handhaving) en strafrecht (opsporing) bevoegdheden kent die de inzet van Web Voyager legitimeren.

Dit onderzoek is in opdracht van de nationale politie uitgevoerd in de periode april-juni door onderzoekers van de Vrije Universiteit Amsterdam. Hoofdstukken 1-3 zijn van de hand van Arno Lodder. Richard Neerhof is verantwoordelijk voor hoofdstuk 4 over bestuursrechtelijk toezicht en handhaving. Matthias Borgers heeft hoofdstuk 5 geschreven. Het slothoofdstuk is van ons drieën.
Het onderzoek richt zich op de bevoegdheden om informatie te vergaren, de verdere verwerking is een onderwerp op zich dat hooguit zijdelings aan de orde is gesteld en zich leent voor vervolgonderzoek.

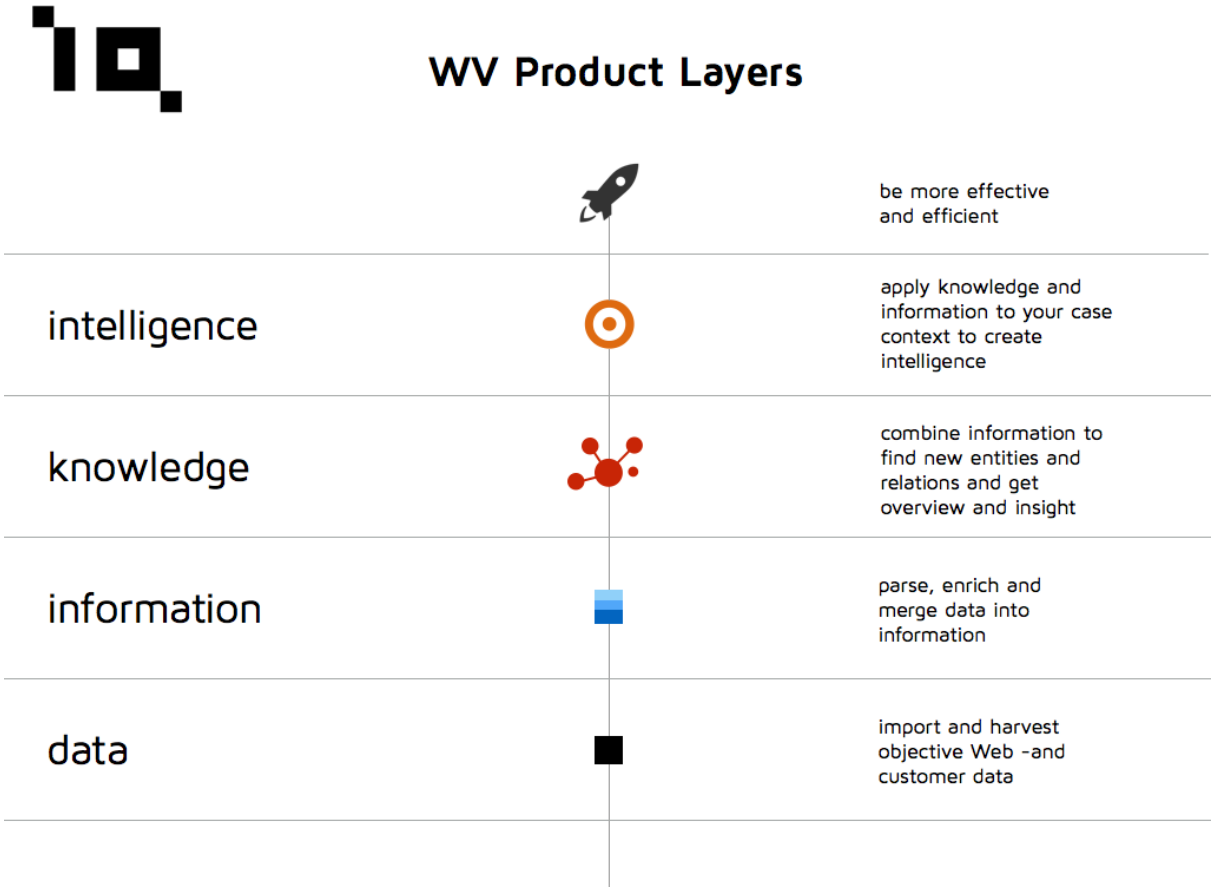
A.R. Lodder, M.J. Borgers & A.R. Neerhof
Amsterdam, juni 2015

Inhoudsopgave[1]

[1] De tekst van hoofdstuk 1, 2, 3 is van de hand van Arno Lodder. Hoofdstuk 4 is geschreven door Richard Neerhof. Matthias Borgers heeft het vijfde hoofdstuk verzorgd. Hoofdstuk 6 is van ons drieën.

1 Inleiding

Dit onderzoek gaat over de proef van de door de politie gebruikte internettoepassing Web Voyager. Waar de ruimtesonde Voyager[2] sinds september 1977 op zeer grote afstand van de aarde de ruimte in kaart brengt, beweegt Web Voyager zich door de virtuele ruimte: Cyber Space. Web Voyager is een zogenaamde webcrawler, in opdracht van de politie ontwikkeld door het Groningse bedrijf Web-IQ.[3] Zoals uit onderstaande afbeelding blijkt, doet Web-IQ net als Google meer dan alleen maar het internet afstruinen en indexeren.



De afbeelding maakt duidelijk dat met iedere stap elementen aan de verzameling worden toegevoegd. De vergaring van informatie, of zoals in dit schema aangeduid met gegevens, vindt plaats in de onderste laag. In de informatie laag worden de gevonden gegevens gecombineerd en verrijkt. In de kennislaag wordt vervolgens de informatie geanalyseerd in de hoop nieuwe aspecten en verbanden te ontdekken. De driedeling gegevens, informatie en kennis is onder andere bekend uit de wereld van kennismanagement.[4] De scheidslijnen tussen de verschillende categorieën is altijd voer voor discussie. Gezien de rijkdom van de op internet aanwezige informatie is moeilijk vol te houden dat enkel gegevens worden verzameld en niet ook informatie, maar gebruik van de term data voor meer dan alleen gegevens is niet ongebruikelijk zoals de momenteel zeer gangbare term 'big data' illustreert. De reden om de term data te gebruiken is om aan te geven dat er door verschillende bewerkingsslagen verrijking van de 'gegevens' plaatsvindt.

[2] http://voyager.jpl.nasa.gov/index.html
[3] http://web-iq.eu, niet te verwarren met WEBIQ, zie http://webiq.nl
[4] M.C.M Weusten, Juridisch kennismanagement: de praktijk, in: A. Oskamp & A.R. Lodder (red.), *Informatietechnologie voor Juristen* (2de druk), Kluwer 2002; M. Apistola & A.R. Lodder, Law firms and IT – towards optimal knowledge management. *Journal of Information, Law and Technology*, 2005(2); M. Apistola, *Advocaat en Kennismanagement* (diss. Amsterdam VU), 2007.

Op het vierde niveau wordt door het toepassen van de gevonden kennis en informatie binnen de organisatie (in casu politie, openbaar ministerie) uitgestegen boven de bekende driedeling gegevens, informatie, kennis tot wat wordt aangeduid met 'Intelligence'.[5] De term intelligence wordt in het Nederlands doorgaans gebruikt in de context van inlichtingen, zoals bij zogenaamde 'Intelligence Agencies' als de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen en Veiligheidsdienst (AIVD).

Intelligence wordt door het lectoraat Intelligence van de Politie Academie omschreven als:[6]

> "informatieverzameling, -analyse en -gebruik bij het nemen van besluiten en het maken van keuzes op operationeel, tactisch en strategisch niveau."

Deze omschrijving sluit aan bij wat business intelligence wordt genoemd: het op een slimme manier verwerken en analyseren van (bedrijfs)gegevens en deze 'opwerken' tot informatie en kennis om zo allerhande bedrijfsprocessen en beslissingen te ondersteunen. Bij Web Voyager wordt intelligence aangewend mede door informatie op internet te verzamelen, dus buiten de eigenlijk organisatie.

De term intelligence wordt binnen de politie breder gebruikt:[7]

> "Intelligence is iets waar iedere agent dagelijks mee te maken heeft. Maar in de praktijk maakt de politie nog veel te weinig gebruik van informatie."

Duidelijk is dat er een samenhang is tussen informatie en intelligence.[8] Kortweg houdt intelligence in dat binnen een organisatie op een slimme manier informatie wordt gebruikt. Web Voyager beoogt hier een bijdrage aan te leveren. Web-IQ prijst hun diensten aan als:[9]

> Find hidden relations and deep insights via our case oriented products. Or collaborate with our team of specialists to combine the big data of the Web with the knowledge of your organisation and build intelligence that really makes a difference.

Dit roept direct juridische vragen op. In beginsel is alles wat op internet staat openbaar,[10] maar dit betekent niet zondermeer dat iedereen met de informatie op internet naar eigen inzicht alles mag doen wat hem of haar goeddunkt. Dit geldt des te meer als de informatie op internet gecombineerd wordt met andere, al dan niet binnen een organisatie aanwezige, informatie. Het recht beoogt gedrag te normeren en ziet in casu op het vaststellen of de door de politie beoogde activiteiten (het gebruiken van door webcrawlen verkregen informatie) toelaatbaar is en zo ja: onder welke voorwaarden. In meer algemene zin bepaalt technologie wat mogelijk is en het recht wat binnen die mogelijkheden toelaatbaar is.[11]

---

[5] Vgl. R.L Ackoff, "From Data to Wisdom", *Journal of Applies Systems Analysis*, Volume 16, 1989 p 3-9.
[6] https://www.politieacademie.nl/kennisenonderzoek/Lectoraten/lectointelligence/
[7] Intelligence, meer dan opsporing – Interview met Mariëlle den Hengst, *Tijdschrift voor Politie* 2009/6 (jrg. 71), p. 21.
[8] Vgl. "De medewerkers van het Real Time Intelligence Center zorgen 24 uur per dag, zeven dagen per week voor actuele informatie.", https://www.politie.nl/themas/politietaken.html
[9] http://www.web-iq.eu/#web-iq
[10] Vgl. Hof van Justitie 13 februari 2014, C-466/12 (Svensson vs. Retriever), overweging 26: "Gelet op het feit dat voor de toegang tot de werken op deze website geen enkele beperkende maatregel werd gehanteerd, was deze website immers vrij toegankelijk voor alle internetgebruikers." en eerder in vergelijkbare zin M.G.A. Egeler & A.R. Lodder, *Computerrecht* 2013/83 (noot bij Rechtbank Den Haag 19 december 2012, NederlandFM) : "Het idee van het internet is toch juist dat nadat content geplaatst is de HELE wereld die content kan benaderen? Welke nieuwe gebruikers kunnen er naast de hele wereldbevolking zich aandienen?"
[11] Vgl. T.C. Wingfield & E. Tikk (2010), Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen, *International Cyber Security Legal & Policy Proceedings*, p. 16-22: "It has been said that politics is the art of the possible, but it would be more correct to say that in nowadays world technology is the art of the possible, just as law is the art of the permissible, and policy is the art of the preferable."

Het internetrecht richt zich op het analyseren van de vraag of en zo ja: op welke wijze aan internet gerelateerde activiteiten genormeerd dienen te worden. De samenleving en zeker de technologie ontwikkelen zich snel. Veelal doen zich ontwikkelingen voor die op het moment dat regelgeving werd vastgesteld niet voorzien waren. Een recent voorbeeld uit het materiële strafrecht is het verbod anders dan handsfree te bellen. Deze strafbepaling is minder dan 15 jaar geleden ingevoerd.[12] Op het moment van invoering was er discussie over de vraag of het handsfree bellen niet net zo afleidend was als bellen met een telefoon in de hand. Dit is aantoonbaar het geval, maar er zijn meer zaken die afleidend zijn en ook niet verboden bij wet zoals het aansteken van een sigaret tijdens het rijden of ruziënde kinderen op de achterbank. Recent is discussie ontstaan over de vraag of het dragen van een smartwatch verboden moeten worden.[13] Op grond van 61a RVV 1990 geldt:

> "Het is degene die een motorvoertuig, bromfiets, snorfiets of gehandicaptenvoertuig dat is uitgerust met een motor bestuurt verboden tijdens het rijden een mobiele telefoon vast te houden."

Je houdt een smartwatch niet vast. Het argument dat het afleidt gaat niet op, dat geldt immers ook voor een telefoon die in een houder staat en waarvan het schermpje steeds oplicht. Het ministerie van Infrastructuur en Milieu geeft echter aan:[14]

> "dat de overheid niet bezig is met een specifieke wetgeving rondom smartwatches. In principe zou Artikel 5 Wegenverkeerswet voorlopig daarvoor genoeg zijn. Dit artikel houdt in dat het sowieso verboden is om je gevaarlijk te gedragen in het verkeer, of iets te doen wat voor gevaar zou kunnen zorgen. Bij de Nationale Politie is het op dit moment nog geen topic waarover wordt gesproken."

Net als er geen specifieke regel voor smartwatches bestaat, is er geen specifieke bevoegdheid op grond waarvan webcrawling activiteiten kunnen worden uitgevoerd.

Op dit moment ontbreekt een overzicht van en inzicht in de juridische aspecten die spelen bij de inzet van webcrawlers zoals Web Voyager in de opsporing en handhaving. De juridische achtergrond waartegen een analyse hiervan in dit rapport zal plaatsvinden betreft:

- internetrecht, in overkoepelende zin;[15]
- bestuursrecht, voor wat betreft toezicht en handhaving;
- strafprocesrecht, voor wat betreft de opsporing.

De vraag die in de analyse aan de orde wordt gesteld is of, en zo ja: in hoeverre, een juridische grondslag kan worden aangewezen voor het door de politie op geautomatiseerde wijze vergaren van informatie op internet ten behoeve van de handhaving en opsporing. Zijdelings kan worden ingegaan op het verrijken van informatie, maar de nadruk ligt op het verzamelen van informatie. De centrale vraag in het rapport is:

> *Onder welke voorwaarden is binnen de handhaving en opsporing het verzamelen van informatie door middel van Web Voyager, meer in het algemeen de inzet van webcrawlers, en het gebruik van die informatie rechtmatig?*

[12] *Stb.* 2002, 67, 4 februari 2002.
[13] Apple Watch Must Be Banned for Drivers, *Huffington Post* 11 mei 2015.
[14] http://www.alwayswith.nl/blog/whats-new/2015/05/smartwatch-verkeer
[15] Vgl. F. Bolhaar e.a., 'Wat is internetrecht?', *Tijdschrift voor Internetrecht* 2014/6. Voor een toegankelijk overzicht van het internetrecht M. van der Linden-Smith & A.R. Lodder, *Jurisprudentie Internetrecht 2009-2015. Een gestructureerde bloemlezing voorzien van commentaar*, Kluwer 2015 en A.R Lodder, *Over de grenzen van het internet. 5 verhalen over recht en onrecht op Facebook, Youtube, Marktplaats, Twitter, Pirate Bay en andere plekken*, Paris 2014.

Binnen het project Web Voyager worden door de nationale politie verschillende pilot-projecten uitgevoerd om praktische resultaten te verkrijgen die inzicht geven in de mogelijkheden van de inzet alsmede het functioneren van webcrawlers. Iron Man is een van die pilot-projecten en richt zich op vuurwapengebruik. Omdat Iron Man ziet op zowel bestuursrechtelijk (wapenvergunningen) als strafrechtelijk optreden van de politie (bijv. schietincidenten) zal dit deelproject als uitgangspunt worden genomen in dit rapport.

Het rapport is verder als volgt opgebouwd. In hoofdstuk 2 wordt ingegaan op de wijze waarop Web Voyager werkt en hoe Web Voyager wordt ingezet in het vuurwapen-project Iron Man.
Hoofdstuk 3 gaat in op de vraag hoe het informatie vergaren op internet zich verhoudt tot de door het Europese Hof van Justitie in 2014 ongeldig verklaarde data retentierichtlijn. De reden om op deze uitspraak in te gaan is dat het hier ook om ongerichte verzamelde grote dataverzamelingen gaat. Niet afzonderlijk wordt stilgestaan bij de door de Europese Commissie tegelijkertijd met de Algemene verordening gegevensbescherming[16] ingediende EU-voorstel Richtlijn bescherming persoonsgegevens bij gebruik door politiële en justitiële autoriteiten.[17] Hoewel onder verwerking ook het verzamelen en vastleggen van gegevens valt, dient voorafgaand aan het verzamelen te worden nagegaan of er binnen de betreffende overheidstaak een bevoegdheid bestaat gegevens te verzamelen. Daarop wordt in dit rapport ingegaan. Een aanvullende reden niet op deze richtlijn in te gaan, is dat het voorstel al dateert van 3,5 jaar geleden en er zeker niet voor 2016 een definitieve tekst is te verwachten die dan op zijn vroegst in 2018 omgezet in nationaal recht zal zijn.
Hoofdstuk 4 richt zich op het toezicht en de handhaving vanuit een bestuursrechtelijke invalshoek.
Hoofdstuk 5 heeft als uitgangspunt het strafprocesrecht en gaat in op de opsporing.
Voortbouwend op hetgeen in hoofdstuk 2-5 aan de orde is gesteld, volgt in hoofdstuk 6 de conclusie en een advies over de wijze waarop vanuit juridisch perspectief Web Voyager in de praktijk al dan niet kan worden ingezet.

[16] Voorstel voor een verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), 25.1.2012, COM(2012) 11 final.
[17] Voorstel voor een richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens, 25.1.2012, COM(2012) 10 final.

2 Webcrawling en Iron Man

2.1 Inleiding

Het is haast niet voor te stellen dat men in de jaren negentig een internetpagina bij een zoekmachine kon aanmelden met het verzoek deze op te nemen in de index omdat veelal pas dan de pagina vindbaar via de zoekmachine werd. Inmiddels worden continue grote delen van het internet geïndexeerd door autonoom opererende webcrawlers. Bij Google leidt een zoekvraag vaak al minuten (seconden?) nadat content op internet geplaatst is tot een treffer. Zelfs de webcrawlers van Google[18] komen echter niet overal, daarvoor is het internet te groot en dynamisch. Er worden keuzes gemaakt, in wat precies gecrawled wordt en hoe vaak informatie ververst moet worden. Ook kunnen webcrawlers zo ingesteld zijn dat deze rekening houden met zogenaamde Robot.txt bestanden, waarmee webpagina's aangeven niet door webcrawlers te willen worden geïndexeerd.

Webcrawling houdt in dat met behulp van een computerprogramma op een methodische en geautomatiseerde manier het wereldwijde web wordt doorgebladerd. Vaak worden gegevens gekopieerd om deze te kunnen verwerken en indexeren voor bijvoorbeeld zoekmachines. Door indexering en bewerking van de verkregen en vastgelegde gegevens kan informatie worden afgeleid die niet of niet snel kenbaar zou zijn voor een willekeurige internetgebruiker. Het systematisch en geautomatiseerd opzoeken, vastleggen en gericht bewerken van op internet beschikbare gegevens is een activiteit die niet op één lijn kan worden gesteld met het 'gewoon' opzoeken van informatie door een individuele internetgebruiker.

Web Voyager is een webcrawler, althans de activiteiten vangen aan met het vergaren van informatie op internet. Het informatie vergaren op internet vindt zonder of met beperkte intelligentie plaats. Vanaf de beginpagina worden alle links gevolgd. Ingesteld kan worden hoe "diep" gezocht wordt. Naarmate dieper gezocht wordt, neemt de hoeveelheid te crawlen pagina's exponentieel toe. Stel dat er gemiddeld 20 links op een pagina staan, dan worden bij één niveau diep 20 pagina's geïndexeerd, bij twee niveau diep 400 pagina's, bij drie niveau 8000 pagina's, bij vier niveau diep 160.000 pagina's en bij 5 niveau diep meer dan 3 miljoen pagina's. In geval er geen beperkingen gesteld worden aan de diepte van indexeren is al snel een groot deel van het internet geïndexeerd. Vanuit verschillende beginpunten gestarte webcrawlers brengen dan ook dataverzamelingen tot stand die naar elkaar toegroeien en uiteindelijk uitmonden in identieke verzamelingen.

In dit hoofdstuk wordt ingegaan op de wijze waarop Web Voyager werkt. Eerst wordt kort ingegaan op enkele rechtelijke uitspraken over het gebruik van internet als bewijsmiddel binnen de straf- en bestuursrechtspraak. Daarna worden de drie verschillende scenario's die het uitgangspunt bij de pilot Iron Man zijn behandeld en tenslotte wordt op de werkwijze binnen Iron Man ingegaan.

2.2 Overheid op internet

Bij de inzet van webcrawlers wordt op systematische wijze het internet doorzocht. Door de overheid wordt al geruime tijd gebruik gemaakt van het internet als informatiebron. Hieronder wordt aan de hand van enkele rechterlijke uitspraken een korte impressie gegeven.

In 2003 werd door advocaat-generaal Jörg in een zaak over een bij verstek gewezen arrest aan de hand van zoekresultaten aangegeven dat niet de juiste spelling van de woonplaats van de verdachte was gebruikt:[19]

[18] Voor een duidelijke beschrijving van de werking van webcrawlers zie M.L. Boonk , *Zeker over zoeken? - Naar een juridisch kader voor verrichtingen van zoeksystemen met betrekking tot via internet beschikbare open content* (diss. Amsterdam VU), Uitgeverij Paris 2013, hoofdstuk 2.
[19] Hoge Raad 2 september 2003, ECLI:NL:PHR:2003:AF8751.

> "Welssborough (een kennelijke verschrijving voor Wellsborough; Welssborough levert op het internet noch onder Google noch onder Yahoo een hit op, waarbij Yahoo zo vriendelijk was te vragen: "We couldn't find any results for "welssborough." Did you mean wellsborough?")."

In een zaak van de Rechtbank Breda uit 2009 ging het over de juridisch relevante grens tussen handhaving en opsporing. Bij de Milieubeheer ambtenaar verscheen tijdens een zoektocht op internet naar een pand een logo van het Hennep-team van de politie op het scherm. Uit de uitspraak wordt niet duidelijk welke internettoepassing gebruikt werd en op welke wijze dit logo verscheen:[20]

> "Op geen enkele wijze is naar het oordeel van de rechtbank zelfs maar aannemelijk geworden dat het door [naam werknemer gemeente] verrichte onderzoek is aangevangen met het doel of mede met het doel om informatie/duidelijkheid te verkrijgen over een hennepkwekerij, een cocaïnewasserij of andere drugsactiviteiten. [naam werknemer gemeente] heeft in zijn verklaringen bij de rechter-commissaris naar het oordeel van de rechtbank duidelijk gemaakt dat het betreffende onderzoek een periodieke controle was in het kader van de Wet milieubeheer en dat hij, *na een eigen zelfstandig onderzoek naar informatie over het pand van medeverdachte [naam medeverdachte] op internet*, alleen contact heeft opgenomen met een medewerker van het Courageteam, omdat het logo van dat team op het scherm was verschenen bij het intypen van de straatnaam van het pand. Uit geen van de bewijsmiddelen blijkt dat hij toen er van uitging of in de veronderstelling verkeerde dat er een hennepkwekerij op dat adres zou zijn. Hij verkreeg door het contact met het Courageteam wel de wetenschap dat er in het verleden een hennepkwekerij op dat adres was aangetroffen."

Binnen de handhaving is op vrij uitputtende wijze inzetten van informatie op internet niet ongebruikelijk. Er zijn gevallen bekend van mensen die op vakantie waren zonder dat door te geven aan de uitkeringsinstantie. Een kiekje op internet van de vakantie kan deze mensen dan in de problemen brengen. Er schijnen zelfs bedrijven te zijn die voor 10 euro "compromitterende" foto's van personen aan uitkeringsinstanties leveren:[21]

> "(...) bedrijven die vervolgens met fotoherkenningssoftware op internet speuren naar alle foto's waar de werkloze op staat (...) waarbij wordt nagegaan bij welke activiteiten de foto's werden gemaakt en in welk eventueel gezelschap de bijstandsgerechtigde zich daarbij bevond."

Heel bont maakte de stratenmaker het die aangaf hooguit een uurtje te kunnen fietsen,[22] maar op internet op een foto stond gemaakt na een wielertocht van 250 kilometer met als onderschrift "trots en voldaan OBN-wielerteam". Ook kon hij nauwelijks zijn bed uitkomen, maar bleek volgens op internet te vinden informatie wel 10 uur te kunnen vliegen en wandeltochten van 80 kilometer te lopen.
In een strafzaak van de Hoge Raad uit 2011 ging het over de vraag of het algemeen bekend moet worden verondersteld dat de afkorting ACAB staat voor All Cops Are Bastards. Bij de vaststelling speelden zoekresultaten een rol:[23]

> "Opmerking verdient nog dat het in dit verband moet gaan om een feit dat in Nederland van algemene bekendheid is. Daartoe is het aantal treffers bij het zoeken in alle, ook anderstalige, internetsites niet zonder meer redengevend. Hetzelfde geldt voor het aantal treffers van de gebezigde zoekmachine waarop het Hof zich heeft beroepen, zonder evenwel te verduidelijken op welke of wat voor soort internetsites die treffers betrekking hebben."

[20] Rechtbank Breda 3 september 2009 (cocaïnewasserij), ECLI:NL:RBBRE:2009:BJ7099.
[21] Zie deze enigszins tendentieuze internetpagina http://www.doorbraak.eu/bijstandsgerechtigden-kijk-uit-big-brother-is-watching-you/
[22] Rechtbank Almelo 21 december 2011 (wielrennende ex-stratenmaker), ECLI:NL:RBALM:2011:BV0428.
[23] Hoge Raad 11 januari 2011 (All Cops Are Bastards), ECLI:NL:HR:2011:BP0291.

Een vrij bekende zaak is die waarin opsporingsambtenaren informatie van Google Earth in de bewijsvoering betrokken.[24] De rechtbank Den Haag nam deze informatie niet mee in de bewijsvoering, maar overwoog ten overvloede:

> "De rechtbank ziet zich aldus gesteld voor de vraag welke betekenis het bepaalde in artikel 2 Politiewet heeft in de digitale wereld. Vooropgesteld zij dat het via Google Earth inzoomen op een of meer plaatsen niet kan worden aangemerkt als het gebruik van bijzondere technische opsporingsmiddelen, nu iedere burger bij het gebruik van het internet, zulks kan doen. (…) Daarbij wordt opgemerkt dat deze bevoegdheid om rond te kijken op een openbaar netwerk niet de bevoegdheid impliceert om stelselmatig voor de uitoefening van de politietaak gegevens van internet te downloaden en in een politieregister op te slaan. In de onderhavige zaak heeft de verbalisante via Google Earth, zijnde een voor iedereen op internet raadpleegbare informatiebron, ingezoomd op de tuin van medeverdachte verdachte, hetgeen een momentopname in de vorm van een fotoafdruk van deze tuin heeft opgeleverd die aan het dossier is toegevoegd. (…)is de rechtbank van oordeel dat (…) niet meer dan een beperkte inbreuk is gemaakt op het recht op de privacy van verdachte, zodat artikel 2 Politiewet 1993 in dit geval een toereikende wettelijke grondslag bood om via Google Earth vast te stellen, of de desbetreffende stoelen zich inderdaad bevonden op het privéadres van verdachte."

De zaak illustreert de door internet verschuivende grenzen in wat openbaar en besloten is. Een tuin is in beginsel een privé terrein, zeker als er schuttingen omheen staan. Door Google Earth komt deze besloten ruimte binnen het bereik van een ieder. Hierbij moet wel de kanttekening worden geplaatst dat niet onder alle omstandigheden het enkele feit dat op een bepaalde website informatie voor een ieder te vinden is, inhoudt dat deze informatie vervolgens ook door de overheid gebruikt mag worden. Steeds zal een afweging moeten plaatsvinden tussen het belang dat gediend is bij het gebruik van deze informatie en de mate van inbreuk op de persoonlijke levenssfeer.

Tenslotte betekende in verschillende zaken[25] de internetgeschiedenis van zoekopdrachten het verschil tussen moord en doodslag. Bij het voorbereiden van een actualiteitencursus Internetrecht viel op dat er in een jaar tijd (2012) dit bij maar liefst drie strafzaken het geval was en plaatste @ARLodder op 17 januari 2013 in reactie op

> Mikko Hypponen @mikko 16 Jan 2013
> Life tip: If you're about to break the law, *do not* make a Google search on how not to get caught. http://www.extremetech.com/extreme/145830-industrial-espionage-amd-files-suit-against-former-employees-for-alleged-document-theft …
> #nVidia
> #AMD
> #Wii

de volgende tweet:

> @mikko Evidence of "premeditated" in case of murder by Google searches in Dutch case law last year in at least three cases

Dit is opgepikt door de journalist Andreas Udo de Heas die er in Computerworld en Webwereld vervolgens een uitgebreid stuk over schreef.[26]

---

[24] Rechtbank 's-Gravenhage 23 december 2011 (opsporing via Google Earth), ECLI:NL:RBSGR:2011:BU9409

[25] Onder andere Rechtbank Zutphen 21 februari 2012 (vuurwapenfilmpje), ECLI:NL:RBZUT:2012:BV6342 en Hof Arnhem 4 mei 2012 (zoekopdrachten als voorbedachte raad), ECLI:NL:GHARN:2012:BW4764.

[26] A.U. de Haes, Google, stille getuige van moord, *Computerworld* 4 april 2013, en A.U. de Haes, Zoekgeschiedenis bewijst steeds vaker moord, *Webwereld* 4 april 2013.

2.3 Drie scenario's

Zoals aangegeven is het internet te uitgebreid om in zijn geheel te indexeren. Behalve dat zijn er ook veel pagina's waarvan op voorhand duidelijk is dat deze voor de politie van geen of hooguit geringe betekenis zijn. Denk hierbij aan pagina's in bijvoorbeeld exotische talen, alsmede een veelheid aan pagina's zonder zelfs maar een indirecte link met Nederland zoals over onschuldige zaken en gebeurtenissen, gekoppeld aan een locatie ver van hier, etc.

Men zou kunnen stellen dat het niet uitmaakt hoeveel (irrelevante) pagina's worden geïndexeerd, zolang men maar op het moment dat men in die verzameling zoekt binnen een redelijk tijdsbestek relevante treffers heeft. Zoals gezegd is het praktisch niet mogelijk het hele internet te indexeren en zal alleen al om die reden een keuze gemaakt moeten worden. Juridisch gezien is de vraag in hoeverre een dergelijke, tot op zekere hoogte integrale kopie van het internet niet als bovenmatig moet worden gezien, mede in het licht van de uitspraak van het Europese Hof van Justitie EU op 8 april 2014 over de ongeldigheid van de Data Retentierichtlijn (Digital Rights Ireland, ECLI:EU:C:2014:238). In het volgende hoofdstuk wordt meer uitgebreid op de verhouding tussen deze uitspraak en het crawlen op internet ingegaan.

2.3.1 Het hele internet[27]

De eerste verzameling internetpagina's is de meest omvattende, namelijk een integrale kopie van (een deel van) het internet. De beperking die in Iron Man wordt gehanteerd is het "Nederlandse" internet. Op drie manieren wordt het crawlen beperkt, namelijk tot:

1. Sites met een Nederlandse domeinnaam (.nl);
2. Sites gehost vanaf een server op Nederlands grondgebied;
3. Sites in (overwegend) de Nederlandse taal.

2.3.2 Fenomeen

In het tweede scenario wordt niet in algemene zin informatie verzameld, maar is het doel een fenomeen in kaart brengen. Onder een fenomeen wordt begrepen een coherente verzameling van voor een crimineel verschijnsel relevante factoren. Voorbeelden van fenomenen zijn fietsendiefstal, mensenhandel, drugshandel, liquidaties, marktplaatsoplichting, etc. Strafrechtelijk kan aansluiting worden gezocht bij het verkennend onderzoek van art. 126gg Sv en het terroristische broertje art. 126hh Sv. In de MvT is aangegeven dat het onderzoek betreft:

> "naar sectoren van de samenleving om vast te stellen of en op welke wijze daarbinnen misdrijven worden beraamd of gepleegd."

Idealiter zou de politie (Dienst Landelijke Informatieorganisatie/ Dienst Regionale Informatieorganisatie) aan integrale 'beeldopbouw' (van het internet) kunnen doen door alle zojuist genoemde en andere fenomenen in kaart te brengen en daar – afhankelijk van opportuniteit en beschikbaarheid van mensen en middelen – verder onderzoek naar te doen. Bij Iron Man is het te bestuderen fenomeen vuurwapens.

Het uitgangspunt is dat het crawlen plaatsvindt op basis van een afgebakende doelstelling die terug te voeren is tot een fenomeen, bijvoorbeeld zoeken op trefwoorden die binnen een fenomeenonderzoek kunnen wijzen op of te herleiden zijn tot een verdachte activiteit.

De werkzaamheden inzake bestudering van het fenomeen die aan de uiteindelijke crawling activiteiten vooraf gaan zijn gedegen. Zo wordt naar literatuur gekeken om te bepalen wat voor een bepaald fenomeen typerende concepten zijn. Deze concepten spelen vervolgens bij het crawlen echter geen rol. De concepten worden in Google ingevoerd en websites die naar boven komen en relevant voor het fenomeen lijken, worden vervolgens als uitgangspunt voor het crawlen genomen. Door deze

[27] Deze en volgende paragrafen zijn een bewerking van materiaal van de Iron Man project groep.

werkwijze ontbeert de binnen Iron Man gebruikte crawling technologie intelligentie om op zinvolle wijze invulling aan fenomeen onderzoek te geven. De crawling activiteiten vinden plaats zonder meeneming van de voor het fenomeen relevante kennis, waardoor er in verhouding veel bijvangst en weinig relevante informatie wordt verzameld. In de kern maakt het hierdoor niet echt uit naar welk fenomeen gecrawled wordt.

2.3.3 Dossier

De meest specifieke vorm is het dossier scenario. Dit komt het meest gericht over. Echter, hier speelt dezelfde beperking van Web Voyager als bij het fenomeen onderzoek genoemd is: het crawlen ontbeert de noodzakelijke intelligentie. Er kan weliswaar met crawlen gestart worden vanaf een bepaalde specifieke pagina gerelateerd aan een concreet object of subject in een aanhangig dossier, maar vervolgens blijft het crawlen beperkt tot het eenvoudigweg volgen van links op de betreffende pagina's.

Het idee is om vanuit de verzamelde informatie toe te werken naar het produceren van een contextdiagram (de werkelijkheid volgens internetsites) en daarna te richten op concrete onderzoekstappen. Het is echter de vraag of het context diagram niet even gemakkelijk kan worden opgesteld op basis van de zeer algemene informatie van het "hele internet". Immers, de verzamelde informatie is behalve het startpunt van de crawlactiviteiten ongericht.

2.4 Werkwijze binnen Iron Man

De praktijkproeven zijn gesplitst in een praktijkproef Opsporing (ter ondersteuning van TGO West in Rotterdam) en een praktijkproef Toezicht (ter ondersteuning van Bijzondere Wetten in Rotterdam).
Bij de Opsporing zijn vijf verdachten van lokale handel in vuurwapens nagelopen. Daaruit is gebleken dat die verdachten – op internet – niet in verband zijn te brengen met vuurwapens. Wel is gebleken dat een van de verdachten mogelijk in verband kan worden gebracht met extremistische ideeën.

Als via het Internet Research Network (iRN)[28] afgeschermd wordt gegoogled dan komen vergelijkbare resultaten rond de vijf verdachten boven. De vraag is echter wat de waarde van deze vaststelling is, nu er binnen Web Voyager geen interessante informatie over deze verdachten naar boven is gekomen, behalve mogelijk de vuurwapen verdachte die gelinkt kon worden aan extremistische ideeën.

Bij Bijzondere Wetten laat een tussentijds resultaat laat zien dat de criteria voor de opbouw van de datasets moeten worden aangepast, in de zin van meer gericht op de legale houders van vuurwapens (sportschutters, jagers en hun respectievelijke verenigingen, alsmede legale wapenhandelaren en legale wapengremia, zoals de KNSA). Voor de Bijzondere Wetten werden de datasets die worden gebruikt voor de Opsporing gebruikt. De daarin gevonden pagina's blijken te ver verwijderd van de legale kant van de vuurwapenzaak (zijnde sportschieten, jagen en legale vuurwapenhandel). Hierdoor worden (potentiële) resultaten gemist. De vraag is echter of dit aan de dataset op zichzelf kan liggen, of dat het eerder het gevolg is van de op de verzamelde informatie uitgevoerde analyse. Het laatste lijkt het geval, in het licht van de ongerichte crawlactiviteiten.

De functionaliteit die bij het zoeken in de dataset geboden wordt, gaat duidelijk verder dan bij een reguliere zoekmachine. Verschillende velden (naam, telefoonnummer, etc.) kunnen worden ingevuld. Voor de opsporingspilot wordt gewerkt aan de mogelijkheid om meerdere verdachten en vooral meer gegevens per verdachte (zoals meerdere locaties of telefoonnummers bij één verdachte) automatisch te kunnen laden en analyseren. Ook worden de analysefuncties verbeterd zodat gerichter kan worden

[28] Zie https://www.nctv.nl/Images/irn-product-sheet_tcm126-444138.pdf: "Het iRN (Internet Recherche & Onderzoek Netwerk) is in 2004 gestart als project bij de Politie Gelderland-Zuid om een mogelijkheid te creëren voor politie afdelingen om op een verantwoorde manier Internet bij opsporing en onderzoek te betrekken. (…) Het project heeft geresulteerd in een, volledig in eigen beheer ontwikkelde, netwerkinfrastructuur voor onderzoek, opsporing, innovatie en ontwikkeling op het gebied van Internetonderzoek."

gezocht op een combinatie van een of meer verdachten met een bepaald onderwerp (bijvoorbeeld ‘antieke wapens’ of voetbalvandalisme).

Web Voyager zorgt ervoor – op het gebied van (de uitvoering van) intelligence en operaties – dat effectiever en efficiënter kan worden opgetreden. Effectiever, doordat een relatieve kleine melding over een vuurwapen (bijvoorbeeld de enkele naam van een verdachte van vuurwapenbezit/-gebruik/-handel) wordt verrijkt met offline gegevens uit de diverse databases van politie en KMar, waarna kan worden gezocht met een relatief rijk profiel in de dataset. Dit kan inhouden dat de trefkans toeneemt in verhouding tot bijvoorbeeld via Google zoeken met enkel de naam van de verdachte. Efficiënter, omdat het proces grotendeels geautomatiseerd is en rechercheurs of informatiecoördinatoren (bij de Opsporing) dan wel vergunningsverstrekkers (bij Bijzondere Wetten) aan de hand van een eenvoudige werkinstructie in beginsel sneller tot een informatiever eindresultaat van een ‘internetzoekactie’ kunnen komen.

De winst door de inzet van Web Voyager ligt op dit moment vooral in de controleerbaarheid en gestructureerdheid van de werkzaamheden. Betrokken partijen bij de bestrijding van illegale vuurwapenhandel in Nederland (politie, KMar, douane en OM) kunnen in plaats van overwegend handmatig en matig verifieerbaar werken, laten zoeken in de dataset aan de hand van een Excel-formulier. Dit zorgt ervoor – op het vlak van accountability en juridische haalbaarheid – dat het proces transparanter wordt en dat het proces beter te verantwoorden is (alsmede herhaalbaar is). Hoewel op zichzelf natuurlijk van belang is dit een aardige bijkomstigheid van het gebruik van Web Voyager, maar niet het eigenlijke doel van de webcrawler.

2.5 Conclusie

De kracht van de technologie van Web Voyager lijkt niet te liggen in een geavanceerde manier van het verzamelen van informatie, hoewel mogelijk de snelheid van indexeren hoog is. Er kunnen dan ook vraagtekens worden gezet bij de relevantie van drie verschillende scenario’s en zelfs bij de relevantie van gevarieerde datasets voor verschillende (deel)onderwerpen. De kracht van Web Voyager zal vooral moeten komen van de fase na de vergaring van informatie, namelijk de analyse en combinatie met al dan niet interne informatiebronnen. Dit aspect kan een rol spelen bij de bepaling van de mate waarin de activiteiten Web Voyager een inbreuk op de persoonlijke levenssfeer vormen. Op zichzelf is denkbaar dat de analytische kwaliteiten dermate goed zijn dat de gemiddelde burger zich niet bespied hoeft te wanen. Dit laatste is immers op zichzelf wel een mogelijk gevaar bij een al te ongebreidelde informatievergaring. In de komende hoofdstukken zullen we ons verder concentreren op de vraag in hoeverre het recht op zichzelf een grondslag kent om informatie via webcrawling te vergaren.

3 Hoe verhoudt dataretentie zich tot webcrawlers

De uitspraak waarin het Hof van Justitie op 8 april 2014 de data rententierichtlijn ongeldig verklaarde verdient nadere bespreking, omdat het hof ingaat op ongebreidelde dataverzamelingen en daar bij webcrawling ook snel sprake van is. De belangrijkste overwegingen uit de uitspraak worden toegelicht en ook wordt kort ingegaan op de uitspraak waarin de Nederlandse rechter in vervolg op het Europese hof de Nederlandse data retentie wetgeving ongeldig verklaarde. Tenslotte wordt voortbouwend op deze behandeling aangegeven welke aspecten van de uitspraken voor webcrawlers relevant zijn.

3.1 De dataretentierichtlijn

De dataretentierichtlijn van de Europese Unie is vastgesteld op 15 maart 2006.[29] Het doel van de richtlijn was om de bewaarplicht van telecommunicatiegegevens binnen de EU te harmoniseren "teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten." (artikel 1 lid 1). Overweging 9 geeft de achtergrond en noodzaak weer:

> "Omdat gebleken is dat de bewaring van gegevens een noodzakelijk en doeltreffend onderzoeksinstrument is voor wetshandhaving in verschillende lidstaten, en met name bij ernstige aangelegenheden zoals georganiseerde misdaad en terrorisme, dient gezorgd te worden dat de bewaarde gegevens beschikbaar zijn voor de wetshandhavingsautoriteiten gedurende een bepaalde periode, onder specifieke voorwaarden."

De telecommunicatiegegevens waar de richtlijn op ziet zijn "verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren." (artikel 1 lid 2). Deze zogenaamde meta gegevens zien niet op de inhoud van de communicatie.

Al van aanvang af was waren er twijfels over de houdbaarheid van de richtlijn in het licht van privacy, hoewel een enkeling tot een positieve conclusie in dezen kwam.[30] Ook werd op 10 februari 2009 de geldigheid van de richtlijn door het Hof van Justitie van de EU (ECLI:EU:C:2009:68) bevestigd:[31]

> *De dataretentie-richtlijn(2006/24) verplicht EU-lidstaten om wetgeving te implementeren betreffende de bewaring van telecom- en internetgegevens met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, waaronder terrorisme. De richtlijn is gebaseerd op artikel 95 van het EG-verdrag. Dit artikel biedt een grondslag voor het nemen van harmoniseringsmaatregelen ten behoeve van de totstandbrenging van de interne markt (zgn. eerste pijler). Ierland, ondersteund door Slowakije, stelt dat de richtlijn nietig moet worden verklaard omdat artikel 95 geen juiste grondslag daarvoor biedt. Ierland stelt dat het 'zwaartepunt' van de richtlijn niet de werking van de interne markt betreft, maar het onderzoeken, opsporen en vervolgen van strafbare feiten. Dergelijke maatregelen moeten worden vastgesteld op grond van de bepalingen van het EU-Verdrag inzake politiële en*

[29] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *PbEG* 13.04.2006, L 105/54.

[30] F. Bignami (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law, Spring 2007*: "Based on a detailed examination of the Directive's legislative history, the paper finds that privacy - as guaranteed under Article 8 of the European Convention on Human Rights and the Council of Europe's Convention on Data Protection - was adequately protected in the Directive."

[31] Uit M. van der Linden-Smith & A.R. Lodder, *Jurisprudentie Internetrecht 2009-2015. Gestructureerde bloemlezing voorzien van commentaar*, Kluwer (4de druk), te verschijnen.

> *justitiële samenwerking in strafzaken (zgn. derde pijler). Het Hof is het niet met Ierland eens. Het stelt vast dat de richtlijn is vastgesteld op de juiste rechtsgrondslag omdat deze overwegend betrekking heeft op de werking van de interne markt. Het Hof verwerpt het beroep van Ierland.*

Nadat al in verschillende landen (zoals Duitsland, Tjechie, Roemenie) de rechter de richtlijn ongrondwettig oordeelde, stelde Ierland 5 jaar na de eerste zaak wederom – op andere gronden - de geldigheid van de dataretentierichtlijn aan de orde, maar nu met succes. Op 8 april 2014 bepaalde het Hof van Justitie EU (Digital Rights Ireland, ECLI:EU:C:2014:238):

> *Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (de Dataretentierichtlijn) is ongeldig.*

3.2 Digital Rights Ireland

3.2.1 De te bewaren gegevens

De gegevens gaan niet over de inhoud van de communicatie, het betreffen zogenaamde verkeersgegevens. Dit zijn meta-data die bij het tot stand brengen van verbindingen gegenereerd worden. Het hof typeert de gegevens in r.o 26 als volgt:

> "(….) Deze gegevens omvatten met name de naam en het adres van de abonnee of de geregistreerde gebruiker, het telefoonnummer van de oproeper en het opgeroepen nummer, alsook een IP-adres voor internetdiensten. Aan de hand van deze gegevens kan met name worden nagegaan met welke persoon en via welke weg een abonnee of geregistreerde gebruiker heeft gecommuniceerd, hoe lang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Bovendien kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee of de geregistreerde gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd."

Deze gegevens kunnen op het eerste gezicht betrekkelijk onschuldig overkomen, maar zonder iets van de inhoud van een communicatie te weten kan veel informatie worden blootgelegd. Dit is een aspect waar het hof nadrukkelijk aandacht aan besteedt in r.o. 27:

> "(…) kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren."

Hierdoor vormt de richtlijn een bijzonder ruime en zware inbreuk op zowel het fundamentele privacy recht (artikel 7 Handvest) als het gegevensbeschermingsrecht (artikel 8 Handvest). Er kan ook een verstikkende werking uitgaan van het ongebreideld opslaan, zeker als de burger niet geïnformeerd wordt over raadpleging van deze informatie (r.o. 37):

> "bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden".

3.2.2 De belangen gewogen

Met de dataretentierichtlijn wordt een doel van algemeen belang gediend (r.o. 44). De gegevens die bewaard dienen te worden, kunnen mogelijk bijdragen aan de opsporing van criminelen of het voorkomen van terroristische acties.

Zoals voor vrijwel alle rechten geldt, heeft ook privacy geen absolute werking. Een inmenging in de privésfeer kan, bijvoorbeeld op gronden aan algemeen belang ontleent, geoorloofd zijn. Zo wordt bij een crimineel die gevolgd wordt of waarvan zijn communicatie wordt afgetapt een inbreuk op zijn privacy gemaakt, maar deze inbreuk wordt, mits de bevoegdheden op basis van de juiste wettelijke gronden zijn ingezet, toelaatbaar geacht. Voor de dataretentierichtlijn "moet worden nagegaan of de vastgestelde inmenging evenredig is." (r.o. 45)

Het hof onderkent in r.o. 51 het grote belang dat met de bewaring van gegevens gemoeid is:

> "van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken".

Het hof vervolgt echter met te stellen dat:

> "een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd."

3.2.3 De betrokkenen

In overweging 58 wordt ingegaan op het feit dat er ook van onschuldigen informatie wordt bewaard. Dit is op zich inherent aan een dergelijke bewaarplicht. De verhouding tussen deze opmerking en de eerdere over het primordiale (essentiële) belang is daarom niet direct duidelijk. De opslag van de gegevens op zichzelf wordt pas van betekenis als er wat met deze gegevens gebeurt.[32] Stel dat er een procedure is die garandeert dat verstrekte gegevens alleen bij specifieke verdenkingen mogen worden opgevraagd en moeten worden vernietigd zodra de verdenking eindigt. In dat geval zal er, eventuele fouten daargelaten, vrijwel nooit informatie over een onschuldige burger worden geraadpleegd. Het punt is hier niet dat iemand die niets te verbergen heeft ook niet te vrezen heeft, want dat gaat uit van de veronderstelling dat er gebruik van informatie gemaakt wordt maar dit nergens toe leidt. Het punt is dat de informatie sowieso niet gebruikt wordt. Dit aspect wordt aangestipt in r.o 59, waarin het hof opmerkt:

> "Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid."

Dit is bijna het tegenovergestelde van een procedure die garandeert dat er geen informatie van onschuldigen wordt verwerkt. In het vervolg van overweging 59 is weer de gedachtegang te vinden dat van verkeersgegevens op het moment dat die opgeslagen wordt al duidelijk is of het in het belang van bestrijding van bijvoorbeeld zware criminaliteit is. Overigens is dit wel verwant aan een ander, belangrijk aspect. Een dergelijke ingrijpende maatregel als de dataretentierichtlijn moet aantoonbaar een bijdrage leveren aan de criminaliteitsbestrijding. Men kan veel technische toepassingen verzinnen die in theorie een bijdrage leveren maar in de praktijk niet. In dergelijk gevallen kan een maatregel beter in zijn geheel achterwege gelaten worden. Kranenborg[33] geeft aan dat niet kan "worden ontkend

[32] De opslag vormt wel een inbreuk op art. 8 EVRM, maar kan gelegitimeerd zijn op basis van art. 8 lid 2 bijvoorbeeld als de verwerking cf. Wbp of Wpg is.Vgl. EHRM 16 januari 2000 (Amann vs. Zwitserland), o.v. 69 "the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding" en vervolgens o.v. 71 "Such interference breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and, in addition, is "necessary in a democratic society" to achieve those aims."

[33] HvJ EU 13-05-2014, C-131/12, SEW 2014/177 (met noot H.R. Kranenborg). Meer algemeen: H.R. Kranenborg, Nieuwe regels voor de bescherming van persoonsgegevens, van belang voor iedereen, *Tijdschrift voor Europees en Economisch recht* 2013/7.

dat het gebruik van communicatiegegevens in sterk toenemende mate een essentiële rol speelt in politieonderzoek en dat het bewaren van dergelijke gegevens (en het gebruik ervan) in beginsel een geschikt middel is om ernstige criminaliteit te bestrijden." De vraag is of Kranenborg gelijk heeft. In de eerste plaats moet het chilling effect dat kan uitgaan van grote dateverzamelingen niet onderschat worden. Mensen gaan zich anders gedragen als ze zich bespied wanen, ongeacht of dit ook daadwerkelijk het geval is (vgl. Panopticon).

De effectiviteit is moeilijk aantoonbaar. In een uitgebreid overzicht van Ferdinandusse, Laheij en Hendriks getiteld *De bewaarplicht telecomgegevens en de opsporing. Het belang van historische telecommunicatie gegevens voor de opsporing* wordt weliswaar van een groot aantal zaken aangeven dat verkeersgegevens een rol hebben gespeeld, maar noch hoe snel de verkeersgegevens na het misdrijf zijn gevraagd (wat om een bewaarplicht te rechtvaardigen belangrijke informatie is) noch hoe essentieel de gegevens waren. De WODC evaluatie uit 2012 laat ook geen overtuigende conclusie horen:[34]

> "(…) de rechter gegevens over telecommunicatieverkeer tussen juli 2012 en februari 2013 in verschillende situaties als bewijsmiddel heeft gebruikt en een plek heeft gegeven in de motivering van het vonnis."

De zinsnede "een plek in de motivering van het vonnis heeft gegeven" lijkt eerder te wijzen op een ondergeschikte dan een doorslaggevende rol. Dit is niet de plaats om dieper in te gaan op de nut en noodzaak van verkeersgegevens, maar een noodzakelijke voorwaarde voor de inzet van webcrawlers is dat dit aantoonbaar tot resultaten leidt.

3.2.4 Waarborgen

Vanwege de verregaande inbreuken is het noodzakelijk dat de regels duidelijk en precies aan geven welke bewaarplicht er nu precies op telecomproviders rust. Daarnaast moet er een garantie zijn dat degenen van wie de gegevens verwerkt worden (r.o. 54):

> "(…) doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens (…)".

Dit geldt eens te meer nu de gegevens automatisch worden verwerkt en (r.o. 55):

> "er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd".

In dit opzicht relevante waarborgen ontbreken in de richtlijn:

> "geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen" (r.o. 60);
>
> "geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan" (r.o. 61);
>
> "geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel" (r.o 62);

[34] G. Odinot *et. Al* (2013), *De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing*, WODC.

> "bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel" (r.o. 62);
>
> "onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan" (r.o. 66).

Van den Hoven van Genderen verwijst in zijn annotatie bij deze uitspraak[35] naar A-G Cruz Vilallon die in zijn advies aangaf dat "gezien de kwetsbaarheid van privacy in onze 'surveillance' society vereist is dat de beperking van deze grondrechten in de wet voldoende gepreciseerd moet zijn." Volgens Van den Hoven van Genderen blijft het doel van de richtlijn staan: retentie van elektronische communicatie verkeers- en locatiegegevens is toegestaan. Dit wel onder de voorwaarde dat aan de hierboven beschreven waarborgen is voldaan. In vergelijkbare zin geeft Koning[36] aan "dat dataretentie niet per se een onevenredig middel in de strijd tegen de georganiseerde misdaad hoeft te zijn." Vervolgens noemt Koning het te algemene karakter en de onvoldoende waarborgen van de dataretentierichtlijn.

3.3 Nederlandse rechter

Bijna een jaar na Digital Rights Ireland, op 15 maart 2015, boog de rechtbank Den Haag zich in kort-geding over de geldigheid van de Nederlandse wetgeving op het gebied van data retentie, waarvan de belangrijkste overwegingen zijn: [37]

> "Anders dan Privacy First cs betogen, kan uit het arrest van het Hof niet worden afgeleid dat een dergelijke ruime bewaarplicht hoe dan ook niet evenredig is ten opzichte van het beoogde doel. Het Hof beoordeelt immers vervolgens de vraag of de Dataretentierichtlijn voldoende waarborgen biedt voor de toegang tot de bewaarde gegevens. Indien het betoog van Privacy First cs juist zou zijn, zou het Hof niet meer aan die vraag zijn toegekomen. Daarbij komt dat het Hof "gelet op een en ander" (*"Having regard to all the foregoing considerations"* , punt 69) oordeelt dat de wetgever de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden. Daaruit volgt dat de opgesomde bezwaren in onderlinge samenhang beschouwd tot dat oordeel hebben geleid.
> In dat verband wordt opgemerkt dat een beperking van de gegevens die moeten worden opgeslagen tot de gegevens van verdachte burgers niet goed denkbaar is met het oog op het doel van de Wbt,[38] de doeltreffende opsporing van zware criminaliteit. In geval van een *first offender* kan immers niet reeds op voorhand een onderscheid worden gemaakt tussen verdachte en niet-verdachte burgers. De noodzaak voor het bieden van waarborgen en garanties ten aanzien van de toegang tot die gegevens is evenwel des te groter nu het gaat om een zeer ruime inmenging, zodat daaraan hoge eisen dienen te worden gesteld."

3.4 Webcrawlers

De uitspraak van het hof van Justitie in Digital Rights Ireland en de Nederlandse rechter bieden interessante aanknopingspunten voor het beoordelen van de rechtmatigheid van de inzet van webcrawlers. De bij dataretentie noodzakelijke waarborgen lenen zich voor toepassing op webcrawlers. Alvorens deze kort te herhalen, gaan wij kort in op de verschillen en overeenkomsten tussen webcrawling en dataretentie.

---

[35] HvJ EU 08-04-2014, C-293/12, *Computerrecht* 2014/76 (met noot R. van den Hoven van Genderen).
[36] HvJ EU 08-04-2014, C-293/12, *EHRC* 2014/140 (met noot M.E. Koning).
[37] ECLI:NL:RBDHA:2015:2498.
[38] Bedoeld wordt Wet bewaarplicht telecommunicatiegegevens.

Een eerste verschil is de partij die de gegevens opslaat. Bij dataretentie is dat een private partij, de telecomprovider. Bij Web Voyager is dat de politie zelf, althans wordt in opdracht van de politie gewerkt. Dit geldt overigens niet voor alle webcrawling activiteiten. De integrale kopie die van sociaal media verkeer wordt bijgehouden door het commerciële bedrijf Coosto wordt gebruikt door politie en andere overheidsinstanties.[39] Fabrini gaf in dit licht overigens eerder dit jaar terecht aan:[40]

> "the distinction between retention of meta-data by private companies rather than by government agencies does not make a real difference, since it is the retention itself that alters the relationship between citizen and government in a way that is inimical [= harmful in effect] to democratic society."

Een tweede verschil is de aard van de informatie. Van internet afkomstige informatie ziet op de inhoud en verkeersgegevens zonderen de inhoud juist uit. Daarmee is van internet afkomstige informatie vanuit een privacy perspectief in beginsel gevoeliger, hoewel de aan enkel meta-data te ontlenen privacygevoelige informatie niet onderschat kan worden, zoals Clayton & Tennis stellen:[41]

> "metadata can be highly intrusive to personal privacy – even more revealing in certain regards than the contents of our communications in some cases"

Verkeersgegevens leggen locatie-informatie bloot (waar was iemand, althans een tot hem/haar behorend apparaat) en communicatie-informatie (met wie, wordt hoe vaak gecommuniceerd). Bij verkeersgegevens kunnen zo verbanden gelegd worden tussen (vermeende) deelnemers aan de communicatie. Er wordt immers vanuit het ene punt informatie uitgewisseld (zoals tekst, spraak) met een ander punt. De op internet aanwezige informatie is zeer divers, zowel qua formaten (beeld, geluid, tekst, etc.) als wat betreft de inhoud. Niet altijd zal informatie aan een bepaalde persoon te koppelen zijn en zeker de verbanden tussen personen zijn minder expliciet dan bij verkeersgegevens.

Door analyse kan Web Voyager uit op internet aanwezige informatie verbanden afleiden, zelfs als die dieper verborgen zijn of voor een doorsnee gebruiker in het geheel niet opgemerkt worden. Deze analytische fase wordt in dit rapport verder niet op ingegaan, maar zal zeker bij het formuleren van waarborgen in het achterhoofd moeten worden gehouden.

Ten slotte kan de oorsprong van de informatie worden genoemd. Anders dan bij verkeersgegevens maakt door crawlers verzamelde informatie al onderdeel van het openbare leven uit. Hierbij moet echter de kanttekening worden geplaatst dat het feit dat iedereen praktisch de mogelijkheid heeft de informatie te raadplegen niet noodzakelijkerwijze volgt dat dit ook juridisch toelaatbaar is. Dit geldt met name voor de bewerking. Het raadplegen van 20-25 afzonderlijke informatiebronnen over een persoon is wat anders, dan deze met elkaar in verband te brengen. Zo kan immers een beeld worden opgebouwd wat onder omstandigheden zelfs meer over iemand kan vertellen dan deze over zichzelf weet.

Bovenstaande verschillen brengen enige nuancering aan in de vergelijkbaarheid van dataretentie met webcrawling. De massaliteit van de verzamelde informatie is echter vergelijkbaar. Gezien de onuitputtelijke informatiebron die het internet is, zal bij webcrawling de mogelijke inbreuk in de

[39] Minister Blok in antwoord op Kamervragen op 5 november 2013 (met kenmerk 2013Z17854): "De politie en negen ministeries (Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Defensie, Economische Zaken, Financiën, Infrastructuur en Milieu, Onderwijs, Cultuur en Wetenschap, Veiligheid en Justitie en Volksgezondheid, Welzijn en Sport) hebben Coosto als leverancier."

[40] F. Fabbrini (2015): Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.. *Harvard Human Rights Journal*, forthcoming.

[41] Newell, B. C., & Tennis, J. T. (2014). Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs. In *iConference 2014 Proceedings* (p. 345–355).

persoonlijke levenssfeer in beginsel groter zijn. Kranenborg wijst hierbij op de actieve houding van de burger in de zin van het op grote schaal vrijwillig beschikbaar maken van informatie. De discussie zal volgens Kranenborg steeds:[42]

> "meer komen te liggen op wat het Hof in de onderhavige zaak een 'aanvullende inmenging' in de fundamentele rechten noemt: de toegang van de bevoegde autoriteiten tot dergelijke gegevens. De onderhavige uitspraak zal in die discussie een belangrijke rol gaan spelen."

Bij dataretentie was er een duidelijke wettelijke grondslag voor het verzamelen en vastleggen van de gegevens. Bij webcrawling is zo'n grondslag voor zover aanwezig veel minder concreet. Daarom staat in dit rapport de vraag centraal of zonder expliciete wettelijke grondslag gegevens kunnen worden vergaard door het internet af te struinen. Bij dataretentie ging het in zekere zin om de vervolgvraag: hoe verhoudt het verzamelen, opslaan en gebruiken van de gegevens zich tot het recht op privacy. Ook als er een wettelijke basis voor het verzamelen bestaat, rijzen privacyvragen met betrekking tot het opslaan en gebruiken van de gegevens. Een belangrijk punt dat uit de uitspraak volgt is dat de opslag op zichzelf, hoe ingrijpend ook, gerechtvaardigd kan zijn, mits er voldoende waarborgen in acht worden genomen.

[42] Kranenborg 2014, zie noot 33.

4 Bestuursrechtelijk toezicht en handhaving

4.1 Inleiding

Bestuursrechtelijke wetgeving verschaft bestuursorganen instrumenten om naleving van bestuursrecht te bewerkstelligen. Deze handhavingsinstrumenten omvatten toepassing van bestuursrechtelijke sanctiebevoegdheden. Zij omvatten ook het *toezicht* dat kan worden uitgeoefend op de naleving van de bij of krachtens de wet gestelde voorschriften en van de bij beschikking individueel opgelegde verplichtingen. Dit hoofdstuk handelt over de vraag of de *verkrijging* van gegevens door middel van webcrawling en of het baseren van sanctiebesluiten op basis van deze gegevens mogelijk is in het kader van bestuursrechtelijke handhaving.

We behandelen eerst algemene regels over toezicht en handhaving door bestuursorganen. Daarna gaan we in op de vraag in hoeverre webcrawling in het kader van toezicht mogelijk is, nu de bevoegdheden met betrekking tot toezicht, evenals de uitoefening ervan, worden begrensd door het bepaalde in de Awb en bijzondere wetten. Vervolgens komt de vraag aan de orde of het mogelijk is handhavingsbesluiten te baseren op informatie die is verkregen door middel van webcrawling. De beantwoording van de vragen is gebaseerd op relevante bepalingen in de Awb, bijzondere wetten en direct werkende mensenrechtenbepalingen en jurisprudentie waarin de uitleg en toepassing van deze bepalingen aan de orde is.

4.1.1 Toezicht en webcrawling: bevoegdheden

Toezicht kan worden omschreven als controle op de naleving van wettelijke voorschriften. Om adequaat te kunnen handhaven, moeten overtredingen kunnen worden geconstateerd en hebben bestuursorganen en ambtenaren bevoegdheden nodig om gegevens te verzamelen die voor de handhaving nodig zijn. Tegen de in het kader van toezicht geconstateerde overtredingen kan worden opgetreden door het bevoegd gezag bijvoorbeeld met een last onder bestuursdwang, een last onder dwangsom of een bestuurlijke boete.

4.1.2 Bevoegdheden op grond van de Awb en bijzondere wetten

In afdeling 5.2 Awb worden algemene regels gegeven voor het uitoefenen van toezicht op de naleving van bij of krachtens enig wettelijk voorschrift gestelde voorschriften. Op grond van art. 5:11 Awb moet onder een toezichthouder worden verstaan

> ‘een persoon, bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift’.

In veel bestuursrechtelijke wetten worden het bevoegd bestuursorgaan bevoegdheden toegekend om een toezichthouder aan te wijzen.[43] In art. 5:15 tot en met 5:19 Awb zijn bevoegdheden en rechten van toezichthouders hebben neergelegd. De toezichthouder is bevoegd:

a. zonder toestemming van de bewoner elke plaats met uitzondering van een woning te betreden, zich zo nodig met behulp van de sterke arm toegang te verschaffen en zich te doen vergezellen door personen die daartoe door hem zijn aangewezen – art. 5:15 Awb;
b. inlichtingen te vorderen – art. 5:16 Awb;
c. inzage te vorderen van een identiteitsbewijs als bedoeld in art. 1 van de Wet op de identificatieplicht – art. 5:16a Awb;[44]

[43] Zo bepaalt bijvoorbeeld artikel 12a van de Instellingswet Autoriteit Consument en Markt dat met het toezicht op de naleving van wettelijke voorschriften dat is opgedragen aan de Autoriteit Consument en Markt zijn belast de bij besluit van de Autoriteit Consument en Markt aangewezen ambtenaren die deel uitmaken van het personeel van deze autoriteit.

[44] Ingevolge art. 2 Wet op de identificatieplicht moet iedereen die de leeftijd van veertien jaar heeft bereikt, op de eerste vordering van een politieambtenaar of een toezichthouder een identiteitsbewijs ter inzage aanbieden. De bevoegdheid tot terinzagevordering is in art. 5:16a Awb neergelegd.

d. inzage te vorderen van zakelijke gegevens en bescheiden, waaronder ook vallen gegevens die langs elektronische weg zijn vastgelegd[15] – art. 5:17 Awb;
e. kopieën te maken van zakelijke gegevens en bescheiden – art. 5:17 Awb;
f. zakelijke bescheiden mee te nemen als ter plekke geen kopieën kunnen worden gemaakt – art. 5:17 Awb;
g. zaken te onderzoeken en monsters te nemen – art. 5:18 Awb;
h. zaken mee te nemen als het onderzoek of de monsterneming niet ter plaatse kan geschieden – art. 5:18 Awb;
i. vervoermiddelen met betrekking waartoe hij een toezichthoudende taak heeft, en hun lading te onderzoeken – art. 5:19 Awb;
j. te vorderen dat een voertuig of een vaartuig door de bestuurder stil wordt gehouden en door de bestuurder naar een door hem aangewezen plaats wordt overgebracht – art. 5:19 Awb;
k. van een bestuurder van een vervoermiddel inzage te vorderen van de wettelijk voorgeschreven bescheiden – art. 5:19 Awb.[45]

Deze bevoegdheden kunnen verstrekkend zijn. Zo kunnen op grond van art. 5:17 Awb ook 'forensic images' worden gemaakt, dat zijn kopieën van het totale bestand van een computer, inclusief gewiste documenten die voor de gebruiker niet meer toegankelijk zijn.[46] In een bijzondere wet kunnen meer bevoegdheden worden gegeven.[47] Bij of krachtens een bijzondere wet kunnen bevoegdheden en rechten overigens ook worden beperkt (art. 5:14 Awb). In art. 5:20, eerste lid, Awb is voorgeschreven dat 'een ieder verplicht (is) aan een toezichthouder alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden'. Een ieder, dus ook iemand die niets van doen heeft met een mogelijke overtreding van een (ook niet tot hem gericht) voorschrift, maar die wellicht wel belangrijke informatie zou kunnen verschaffen, kan in beginsel geconfronteerd worden met de uitoefening van bevoegdheden door een toezichthouder. De medewerking dient te geschieden op straffe van overtreding van art. 184 Sr.[48]

De toezichtbevoegdheden en -rechten kunnen worden uitgeoefend in situaties waarin in het geheel nog geen verdenking van een overtreding van voorschriften bestaat. Het betreft dus uitdrukkelijk geen (strafrechtelijke) opsporingsbevoegdheid.

---

[45] Zie over deze bevoegdheden uitgebreid: A.B. Blomberg, Integrale handhaving van het milieurecht (diss. VU), Den Haag: BJu 2000, p. 63-70; O.J.D.M.L. Jansen, Het handhavingsonderzoek (diss. UvA), Nijmegen: Ars Aequi Libri 1999, p. 18-39.

[46] Vzngr. Rb. Den Haag 9 april 2003, AB 2003, 199 m.nt. O. Jansen, KG 2003, 117 (HBG Civiel BV).

[47] Zo bepaalt bijvoorbeeld artikel 12b van de Instellingswet Autoriteit Consument en Markt dat de daartoe aangewezen toezichthoudende ambtenaren bevoegd zijn om bedrijfsruimten en voorwerpen te verzegelen, voor zover dat voor de uitoefening van de in artikel 5:17 van de Algemene wet bestuursrecht bedoelde bevoegdheden redelijkerwijs noodzakelijk is en zij deze bevoegdheden zo nodig uitoefenen met behulp van de sterke arm.

[48] Het opzettelijk niet voldoen aan een bevel of vordering van een toezichthouder is een misdrijf. In de Awb is geen bevoegdheid tot toepassing van bestuurlijke sancties verschaft voor het afdwingen van medewerking bij toezicht. In een enkele bijzondere wet is een dergelijke bevoegdheid wel toegekend. Zie bijvoorbeeld art. 12m, eerste lid, aanhef en onder b, Instellingswet Autoriteit Consument en Markt voor een boetebevoegdheid en art. 5.14 Wet algemene bepalingen omgevingsrecht voor een bestuursdwangbevoegdheid bij overtreding van artikel 5:20, eerste lid, Awb. Alleen personen die uit hoofde van ambt, beroep of wettelijk voorschrift verplicht zijn tot geheimhouding (artsen, notarissen, advocaten), kunnen het verlenen van medewerking weigeren, voor zover dit uit hun geheimhoudingsplicht voortvloeit (art. 5:20, tweede lid, Awb). Er geldt verder geen andere beperking voor degenen van wie door de toezichthouder medewerking kan worden gevorderd dan art. 5:13 Awb, tenzij in de bijzondere wet de kring van degenen bij wie deze medewerking kan worden gevorderd, nader is beperkt. Zo moet de accountant van een omroepinstelling door hem vervaardigde controledossiers overleggen als een toezichthouder van het Commissariaat van de Media dit redelijkerwijs kan vorderen. Hof 's-Gravenhage 30-12-2004, AB 2006, 301 m.nt. O. Jansen (commissariaat voor de Media/Ernest & Young Registeraccountants). Zie voor een beperking van inlichtingenvordering bij werknemers op grond van het zwijgrecht van de verdachte onderneming echter Rb. Rotterdam 11 juli 2006, AB 2007, 35 m.nt. O. Jansen (Heijmans Beton- en Waterbouw BV); Rb. Rotterdam 7 augustus 2003, AB 2004, 92 m.nt. O. Jansen (Texaco).

4.1.3 Webcrawling

Met behulp van webcrawling kunnen overtreders en overtredingen gemakkelijker op het spoor worden gekomen. Webcrawling kan worden gebruikt om tot risicoprofielen te komen, die de basis vormen van meer gerichte controles op naleving van voorschriften die bij of krachtens de wet zijn gesteld. Dit betekent dat de kenmerken van die groep worden beschreven waarbij grotere kans bestaat dat het onderzoek leidt tot het vaststellen van overtredingen. Daarbij valt in het bijzonder te denken aan groepskenmerken die bestaan uit feitelijk gedrag.[49]

Worden met webcrawling de bevoegdheden voor toezicht die zijn neergelegd in de Awb en bijzondere wet niet ongeoorloofd uitgebreid tot buitenwettelijke? Die vraag lijkt te veronderstellen dat informatie over de naleving van wettelijke voorschriften (in het kader van bestuursrechtelijke informatie) alleen kan worden verkregen via uitoefening van de bevoegdheden die de daartoe aangewezen toezichthouder op grond van de Awb of de bijzondere wet heeft. Dat ook andere informatie over naleving van het gestelde bij of krachtens de wet mag worden verkregen dan met uitoefening van deze bevoegdheden en dat die informatie mede de grondslag kan vormen voor een sanctiebesluit, lijkt niet ter discussie te staan. De in de Awb en de bijzondere wet neergelegde bevoegdheden van een toezichthouder zijn bedoeld als instrumenten die het bestuur kan inzetten en begrenzen de uitoefening ervan, maar lijken het gebruik van op andere wijze dan via de uitoefening van deze bevoegdheden verkregen informatie niet bij voorbaat uit te sluiten. Anders dan de opsporing in het strafrecht geldt voor het verzamelen van informatie met het oog op het vaststellen of wettelijke voorschriften worden nageleefd door of namens het tot handhaving van deze voorschriften bevoegde bestuursorgaan niet, dat er een toereikende wettelijke grondslag moet zijn willen de resultaten van webcrawling kunnen worden gebruikt bij besluitvorming over oplegging van een bestuurlijke sanctie.

Zo kan informatie worden verkregen door en op basis van klachten van burgers over bepaalde overtredingen. Die informatie is dan vervolgens startpunt voor nader onderzoek waarbij gebruik wordt gemaakt van toezichtsbevoegdheden uit de Awb of de bijzondere wet. Ook informatie die via webcrawling is verkregen zou een startpunt kunnen zijn voor nader onderzoek waarbij gebruik wordt gemaakt van de bevoegdheden in de Awb. Dat is op zich niet wettelijk uitgesloten.

4.2 Toezicht en webcrawling: de betekenis van beginselen van behoorlijk bestuur

4.2.1 Ongereguleerd?

Webcrawling kan door bestuursorganen worden ingezet bij de controle op naleving van wettelijke voorschriften. Zoals gezegd is de toepassing ervan niet goed onder te brengen bij een van de bevoegdheden in artikel 5:15 tot en met 5:19 van de Awb en evenmin – op het eerste gezicht – bij bevoegdheden die toezichthouders op grond van bijzondere wetten kunnen hebben. De vraag is wel of inzet van webcrawling ter ondersteuning van de genoemde toezichtsbevoegdheden niet aan bepaalde grenzen is gebonden en zo ja, welke dat zijn. Hierop is geen pasklaar antwoord. Voor de beantwoording kan te rade worden gegaan bij het bepaalde in de Awb, bijzondere wetten en direct werkende mensenrechtenbepalingen. We bespreken de bepalingen die mogelijkerwijs relevant zijn.

4.2.2 Algemene beginselen van behoorlijk bestuur, regels voor toezicht en webcrawling

Op de *toezichtshandelingen* is hoofdstuk 2 Awb van toepassing. Toezichtshandelingen zijn veelal feitelijke handelingen en geen besluiten in de zin van de Awb.[50] Zodoende is hoofdstuk 3 op die handelingen in beginsel slechts gedeeltelijk en geclausuleerd van toepassing. Ingevolge schakelbepaling art. 3:1, tweede lid, Awb zijn de afdelingen 3.2 tot en met 3.4 Awb namelijk op

[49] Bunt, S. en M. van der Aalst, *Risicosturing bijstandsfraude inventarisatie van methodieken* Leiden: Ministerie van Sociale Zaken en Werkgelegenheid/ Research voor Beleid 2003, i.h.b. p. 9.
[50] CBB 21 juli 1998, AB 1998, 437 m.nt. Van der Veen, AB Klassiek 2003, 43 m.nt. Michiels (Bosque Teca Verda); Vzngr. Rb. Rotterdam 10 januari 2008, AB 2008, 122 m.nt. O. Jansen (GoodWood Investments B.V).

andere handelingen van bestuursorganen dan besluiten van overeenkomstige toepassing, voor zover de aard van deze handelingen zich daartegen niet verzet.[51] Daarnaast gelden voor de toezichthouder de ongeschreven beginselen van behoorlijk bestuur. In afdeling 5.2 Awb zijn meer specifieke regels opgenomen ter bescherming van de rechtspositie van de burger, die immers de kans loopt dat hij in de greep van de toezichthouder terechtkomt. De toezichthouder moet zich ingevolge art. 5:12 Awb in ieder geval legitimeren voordat hij van zijn omvangrijke en ingrijpende machtsmiddelen gebruik maakt. Een andere beperking staat in art. 5:13 Awb: 'Een toezichthouder maakt van zijn bevoegdheden slechts gebruik voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is.' Zo mag de bevoegdheid om plaatsen te betreden of om zaken en vervoermiddelen te onderzoeken niet worden uitgeoefend om 'inkijkoperaties' uit te voeren, dat wil zeggen operaties waarvan betrokkenen niet op de hoogte zijn. De uitoefening van deze bevoegdheid mag evenmin zo ver gaan dat de betreden plaatsen worden doorzocht. [52]

Webcrawling kan feitelijk handelen van een bestuursorgaan zijn, maar is geen toezichtshandeling als bedoeld in titel 5.2 Awb. Het gaat niet om uitoefening van één van de in die titel of in een andere wet neergelegde bevoegdheden (zoals inlichtingen vorderen, het betreden van plaatsen, en dergelijke). Artikel 5:13 is dus niet van toepassing hierop. Echter, gelet op art. 3:1, eerste lid, Awb zijn onder meer de artikelen 3:2 tot en met 3:4 Awb hierop van toepassing, voor zover de aard van de handeling zich daartegen niet verzet. Zo zal een bestuursorgaan dat webcrawling gebruikt als instrument in het kader van handhaving daarbij het zorgvuldigheidsbeginsel (art. 3:2 Awb) en het evenredigheidsbeginsel (art. 3:4, tweede lid, Awb) in acht moeten nemen.[53] Het gebruik van de via webcrawling verkregen informatie moet voldoen aan eisen van zorgvuldigheid. De gevolgen van webcrawling moeten voor de belanghebbende niet onevenredig zijn ten opzichte van de daarmee te realiseren doelen.

De algemene beginselen van behoorlijk bestuur, in het bijzonder het zorgvuldigheidsbeginsel, kunnen een bijzondere invulling krijgen bij webcrawling. De eisen bij gebruik van webcrawling in het kader van toezicht en handhaving door bestuursorganen worden gesteld zijn niet zo streng als die aan het gebruik ervan in het kader van strafrechtelijke opsporing. Verwerking van politiegegevens is alleen toegestaan wanneer die gegevens rechtmatig zijn verkregen, en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (artikel 3 lid 2 Wet politiegegevens). Voor verwerking van andere gegevens dan die door de politie verkregen, in het kader van uitoefenen van toezicht als hier bedoeld, bestaan geen duidelijke rechtsregels. Bij besluitvorming over de oplegging van een bestuurlijke sanctie wordt regelmatig gebruik gemaakt van bewijs dat in het kader van een strafrechtelijk onderzoek is verkregen. Dit bewijs kan onrechtmatig zijn verkregen. In het kader van opsporing kunnen via webcrawling gegevens zijn verzameld, terwijl daarvoor geen wettelijke basis bestond en die niet kunnen worden gebruikt als bewijs in een strafproces.[54] De vraag is of het gebruik van dit bewijs ter onderbouwing van een bestuurlijke sanctie geoorloofd is. Volgens de jurisprudentie van de belastingkamer van de Hoge Raad en de hoogste bestuursrechters is er geen rechtsregel die elk gebruik verbiedt van (strafrechtelijk) onrechtmatig verkregen bewijsmiddelen in bestuurlijke besluitvorming. Het gebruik van deze bewijsmiddelen is in elk geval niet ongeoorloofd als de bewijsmiddelen jegens de belanghebbende niet op onrechtmatige wijze zijn verkregen. Als het bewijs jegens de belanghebbende op (strafrechtelijk) onrechtmatige wijze is verkregen, behoeft dit voor het bestuursorgaan geen beletsel te zijn om daarvan gebruik te maken. Dan moet met inachtneming van alle relevante omstandigheden worden beoordeeld of wordt

[51] Zie voor bijvoorbeeld de betekenis van het zorgvuldigheidsbeginsel voor controles of aan de geldende geluidvoorschriften wordt voldaan: ABRvS 20 juli 2005, JOM 2007, 555 (jongerencentrum Pitstop). Zie meer over de toetsing van toezichthandelingen die hebben geleid tot handhavingsbesluiten: Vzngr. Rb. Rotterdam 18 oktober 2005, Gst (2006) 7261.152 m.nt. Rogier (Hajenius en Ritmeester).

[52] PG Awb III, p. 349-350; Kamerstukken II 1995/96, 24 617, nr. 3, p. 8.

[53] Zie ook PG Awb III, p. 338.

[54] Meer gangbare voorbeelden. Er kan zonder toestemming van belanghebbende bewijsmateriaal zijn verkregen tijdens een bij hem verrichte huiszoeking terwijl deze zonder het vereiste verlof van het bevoegde orgaan (officier van justitie of advocaat-generaal ingevolge art. 3, eerste lid, Algemene wet op het binnentreden) is gedaan, of er kan een legitimatie door een politieambtenaar achterwege zijn gelaten.

gehandeld in strijd met enig algemeen beginsel van behoorlijk bestuur, meer in het bijzonder met het zorgvuldigheidsbeginsel, door van het strafrechtelijk onrechtmatig verkregen bewijsmiddel gebruik te maken.

Er is volgens de Hoge Raad in het algemeen geen strijd met algemene beginselen van behoorlijk bestuur als het bestuursorgaan zonder dat de onrechtmatige handelingen hadden plaatsgevonden, zonder wettelijke belemmering van de betreffende gegevens kennis had kunnen nemen. De reden is dat door de mogelijkheid van rechtmatige bewijsverkrijging door belanghebbende geen schade is geleden als gevolg van de onrechtmatige bewijsverkrijging. De rechtmatigheid van de alternatieve bewijsverkrijging moet vaststaan. Zo laat zich denken dat in het kader van opsporing via webcrawling onrechtmatig verkregen bewijs toch in een kader van bestuurlijke besluitvorming kan worden gebruikt omdat de informatie op die wijze wel door het bestuursorgaan kon worden verkregen.

Gebruik van een onrechtmatig verkregen bewijsmiddel is niet toegestaan, indien het is verkregen op een wijze die zozeer indruist tegen hetgeen van een behoorlijk handelende overheid mag worden verwacht, dat dit gebruik onder alle omstandigheden ontoelaatbaar moet worden geacht.[55] Uitsluiting van strafrechtelijk onrechtmatig verkregen bewijs is echter slechts in uitzonderlijke gevallen aan de orde.[56]

Het zorgvuldigheids- en evenredigheidsbeginsel stelt grenzen aan het gebruik van het instrument webcrawling, maar het is niet duidelijk hoe strak die zijn. Gelet op het voorafgaande (gebruik van strafrechtelijk verkregen onrechtmatig bewijs), ligt het in de reden onderscheid te maken tussen de soort sancties waarvoor de via webcrawling verkregen gegevens worden gebruikt. Voor een bestraffende bestuurlijke sanctie zouden voor wat betreft gebruikmaking van gegevens via webcrawling verkregen dezelfde beperkingen moeten gelden als die welke gelden voor strafvervolging. Deze stellingname is deels te baseren is op het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (zie hieronder).

4.2.3 Het EVRM en gebruik van webcrawling in het kader van bestuurlijke handhaving

Het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) stelt beperkingen aan het optreden door de overheid, waaronder bij controle op naleving van wettelijke voorschriften. Hieronder wordt nagegaan of en zo ja welke grenzen het EVRM zou kunnen stellen aan het gebruik van webcrawling in het kader van bestuurlijke handhaving.

4.2.3.1 Art. 6 EVRM

Aangenomen moet worden dat bewijsverkrijging waarbij de waarborgen van art. 6 EVRM voor een criminal charge niet in acht zijn genomen, niet mag worden gebruikt voor een bestuurlijke sanctie die als een criminal charge is aan te merken, in het bijzonder de bestuurlijke boete. Een andere opvatting

[55] HR 1 juli 1992, NJ 1994, 621 m.nt. Scheltema, BNB 1992, 306 m.nt. Den Boer (Zwitserse Aktiengesellschaft), r.o. 3.2.2 - 3.2.5. De formule van dit arrest is ook aan te treffen in jurisprudentie van de bestuursrechter: ABRvS 18 februari 2003, AB 2003, 328 m.nt. Sewandono (strafrechtelijk onrechtmatig verkregen bewijs III); ABRvS 4 februari 2000, AB 2000, 242 m.nt. Damen, JB 2000, 72, Gst. (2000) 7120.3 m.nt.Hennekens (strafrechtelijk onrechtmatig verkregen bewijs II); CRvB 28 november 1995, JB 1995, 329, RSV 1996, 89, Gst. (1996) 7042.5 m.nt. De Bruijn (strafrechtelijk onrechtmatig verkregen bewijs I).
Zie: H.E. Bröring, De bestuurlijke boete, Deventer: Kluwer 2005, p. 175. Zie verder over het gebruik van bestuursrechtelijk onrechtmatig verkregen bewijs: ABRvS 12 april 2006, AB 2006, 281 m.nt. Michiels (weigering jachtakte korpschef Groningen); CRvB 11 april 2007, AB 2007, 149 m.nt. Bröring (onaangekondigd huisbezoek); CRvB 24 juni 2008, AB 2008, 286 m.nt. Bröring (vergelijking cliëntenbestand bijstand met bestand RDW); vgl. M.C.D. Embregts, *Uitsluitsel over bewijsuitsluiting* (diss. UvT), Dordrecht: Kluwer 2003, p. 287-293, die betoogt dat gebruik van bestuursrechtelijk verkregen bewijs eerder is uitgesloten. Zie over de vraag of gebruikmaking van onrechtmatig verkregen bewijs dat ook op rechtmatige bewijs had kunnen worden verkregen, onder omstandigheden zozeer kan indruisen tegen hetgeen van een behoorlijke overheid wordt verwacht, Embregts 2003, p. 280-281.

[56] HR 9 september1992, BNB 1992, 366 m.nt. Den Boer (onrechtmatig verkregen bewijs II); HR 9 september 1992, BNB 1992, 367 m.nt. Den Boer (onrechtmatig verkregen bewijs I); HR 12 maart 1997, BNB 1997, 146c m.nt. Wattel (schending verschoningsrecht).

zou (onder meer) een doorkruising opleveren van de waarborgen die in artikel 6 EVRM (en in Sv en de Awb) zijn neergelegd voor criminal charges.[57] Meer dan tot nu toe zou bij de beantwoording van de vraag naar de toelaatbaarheid van gebruikmaking van onrechtmatig verkregen bewijs een onderscheid moet worden gemaakt tussen herstelsancties en bestraffende bestuurlijke sancties.[58] Als via webcrawling bewijs gelet op art. 6 EVRM onrechtmatig bewijs is verkregen, zou dat dus niet ten grondslag moeten kunnen worden gelegd aan bestuurlijke bestraffende sanctie. Het feit dat informatie die via webcrawling is verkregen als onrechtmatig bewijs geldt in het kader van strafvervolging of bestuurlijke bestraffing, hoeft op zich niet in de weg te staan aan gebruik ervan in het kader van herstelsancties. Dat laat echter onverlet dat gebruik van webcrawling in het kader van alle bestuurlijke handhaving aan grenzen onderhevig kan zijn op grond van art. 8 EVRM.

4.2.3.2 Art. 8 EVRM

Ingevolge art. 8, eerste lid, EVRM heeft een ieder recht op eerbiediging van de persoonlijke levenssfeer. Art. 8, tweede lid, EVRM laat alleen inbreuken toe die voorzien zijn bij wet en die een toegelaten doel beogen te bereiken, zoals het economisch welzijn van het land. Een inbreuk dient gelet op het toegelaten doel evenredig te zijn. Voor de evenredigheid is van belang of een adequaat systeem van rechtsbescherming en controle bestaat om misbruik te voorkomen

Het toepassingsbereik van artikel 8 EVRM strekt zich blijkens de rechtspraak van het EHRM uit tot het verzamelen en verwerken van persoonsgegevens.[59] De informatie die wordt gebruikt bij webcrawling is op het publieke internet te vinden en dus voor een ieder raadpleegbaar. Zij kan ook gevoelig zijn, maar een inbreuk op het recht op bescherming van de persoonlijke levenssfeer in art. 8 EVRM kan op zich niet zijn gelegen in het feit dat deze informatie wordt gebruikt. Toch zou ook, met gebruik making van webcrawling door toezichthouders en bestuursorganen in het kader van bestuurlijke handhaving een inbreuk kunnen worden gemaakt op de persoonlijke levenssfeer van een persoon (als bedoeld in art. 8 EVRM). Deze kan zijn gelegen in het feit dat deze openbare gegevens (van overheidswege) systematisch en geautomatiseerd zijn verzameld, waarbij die gegevens – al dan niet na bewerking daarvan – informatie omtrent een persoon blootleggen, die met een gewone zoekopdracht op internet niet zou zijn verkregen en die gegevens vervolgens van doorslaggevende betekenis zijn geweest voor het nemen van een bepaald besluit jegens deze persoon. De vraag is nu onder welke omstandigheden de verkregen informatie en het gebruik ervan door de overheid zodanig is dat sprake is of kan zijn van een inbreuk van de persoonlijke levenssfeer en van een zodanige inbreuk dat artikel 8 EVRM is geschonden.

Als het gaat om beantwoording van de vraag welke gegevens wel of niet worden beschermd door artikel 8 EVRM toetst het EHRM of het privéleven van een individu door de verwerking/gebruikmaking van de gegevens wordt geraakt.[60] Daarbij zij opgemerkt dat het professionele en handelsleven van een persoon niet van de persoonlijke levenssfeer wordt uitgezonderd. Hiertoe behoort het recht om (al dan niet) zakelijke relaties aan te gaan met anderen. Bovendien is het niet goed mogelijk om de persoonlijke levenssfeer te onderscheiden van de professionele levenssfeer.[61] Verder is volgens het Hof in art. 8 eerste lid, EVRM uitdrukkelijk aan rechtspersonen het grondrecht op respect voor de 'domicile' toegekend.[62]

Aangenomen mag worden dat het antwoord op de vraag of sprake is van een inbreuk op het recht als bedoeld in art. 8, eerste lid, EVRM (ook) in de context van gebruik van webcrawling door

[57] Vgl. F.C.M.A Michiels & B.W.N. de Waard, Rechterlijke toetsing van bestuurlijke juridische sancties, Den Haag: BJu 2007, p. 113-114; Embregts 2003, p. 334-338.
[58] Zie onder meer: Embregts 2003, 283-294.
[59] Zie o.a. EHRM 2 augustus 1984, app. no. 8691/79 (Malone v. The United Kingdom), par. 84, respectievelijk o.a. EHRM 26 maart 1987, app. no. 9248/81 (Leander v. Sweden), par. 48.
[60] Vgl. EHRM 25 september 2001, app. no. 44787/98 (P.J. and J.H. v. The United Kingdom), par. 42.
[61] EHRM 16 december 1992, Series A vol. 251–B, NJ 1993, 400, m.nt. Dommering (Niemetz), r.o. 29-31; EHRM 30 maart 1989, Series A vol. 152, NJ 1991, 522, m. nt. Dommering (Chappell) .
[62] EHRM 16 april 2002, AB 2002, 277, m.nt. O.J.D.M.L. Jansen . NJ 2003, 452, m.nt. Dommering, EHRC 2002, 46 m.nt. Janssen (Cola Est).

bestuursorganen afhankelijk is van de aard van de informatie die wordt verkregen, in het bijzonder of een min of meer compleet beeld ontstaat van bepaalde – aan een zekere sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen rakende – aspecten van het persoonlijke leven van een persoon.[63] Het antwoord op de vraag of hiervan sprake is, wordt in sterke mate bepaald door concrete omstandigheden.[64] Het gebruik maken van dit instrument zal geschieden zonder dat betrokkene ervan weet. Dat is op zich geen inbreuk.

Voor zover webcrawling een instrument vormt om op basis van risicoprofiel controles op naleving van bij of krachtens de wet gestelde voorschriften uit te voeren, kan worden opgemerkt dat dit feit op zich geen schending van art. 8 EVRM oplevert. Het is overigens vaste jurisprudentie van de Centrale Raad van Beroep dat bij de inzet van de algemene onderzoeksbevoegdheid het toepassen van risicoprofielen geoorloofd is.[65]

Als in een concreet geval wél sprake is van een inbreuk, is de vervolgvraag of deze gerechtvaardigd is. Volgens vaste rechtspraak is een inbreuk op de persoonlijke levenssfeer van een individu op grond van artikel 8 lid 2 EVRM (slechts dan) gerechtvaardigd indien die inbreuk (1) noodzakelijk is in een democratische samenleving ("necessary in a democratic society") voor (2) verwezenlijking van één van de in deze bepaling genoemde doelen, waaronder de nationale veiligheid en (3) in overeenstemming is met het recht ("in accordance with the law").

Hoe toe te passen bij een inbreuk die is ontstaan door webcrawling? Wanneer is de inbreuk geoorloofd?

1. De persoonlijke levenssfeer van de betrokkene mag niet onevenredig worden geschaad (proportionaliteit, 'pressing social need'). Het gaat om de vraag of de inmenging noodzakelijk is in een democratische samenleving, proportioneel is – de beperking op het recht mag niet onevenredig zijn in verhouding tot het nagestreefde doel – en voldoet aan de eis van subsidiariteit – het nagestreefde doel mag niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt. Uit de eis van proportionaliteit zal volgen dat naarmate een inbreuk op de privacy groter is het belang van gebruik van webcrawling en van de daarmee verkregen gegevens in het kader van bestuurlijke handhaving concreter moet zijn.
   Uit het voorgaande volgt dat steeds een belangenafweging moet worden gemaakt. Het ligt weinig voor de hand dat voor webcrawling door de wetgever de figuur van voorafgaande rechterlijke machtiging wordt ingevoerd (uitvoeringslasten, belemmering van effectief onderzoek, etc). Er moet bij webcrawling echter wel een adequate rechterlijke toetsing achteraf kunnen plaatsvinden. De rechtmatigheid naar nationaal recht en de noodzakelijkheid van het verzamelen van de informatie, dus ook die door middel van webcrawling, moet vast komen te staan en door de nationale rechter kunnen worden getoetst. Als die toetsing in voorkomende gevallen niet door de rechter kan worden uitgevoerd, is de werkwijze niet proportioneel.[66] Verder komt de Staat bij een inbreuk op artikel 8 EVRM ten aanzien van een rechtspersoon een grotere appreciatiemarge toe bij de beoordeling van de proportionaliteit van een dergelijke inbreuk dan in geval van een natuurlijke persoon.[67] Echter, lidstaten zouden bij beperkingen op bescherming van de levenssfeer

[63] Vgl. hoofdstuk 5 in dit rapport; zie hieromtrent ook de noot van Borgers onder HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, onder punt 2.
[64] Zie o.m. EHRM 25 september 2001, NJ 2003, 670, m.nt. EJD, EHRC 2001/76, m.nt. Spronken (P.G. en J.H., t. Verenigd Koninkrijk), r.o. 56-60.
[65] Zie onder meer: Centrale Raad van Beroep 14 april 2015, RSV 2015/104, ECLI:NL:CRVB:2015:1231, r.o. 4.2; Centrale Raad van Beroep 14 april 2015, ECLI:NL:CRVB:2015:1229 , r.o. 4.3.3.
[66] In de uitspraak wordt de term proportioneel gebruikt, maar qua strekking kan ook de term rechtmatig worden gebezigd. EHRM 2 oktober 2014, AB 2015, 29, m.nt. T. Barkhuysen en M.L. van Emmerik (Delta Pekarny t. Tsjechië). Vgl. CBB 11 februari 2010, AB 2010, 243, m.nt. I. Sewandono (over verwerking medische en andere persoonsgegevens, zoals die zich bij een ziekenhuis bevinden door de NZA en gebruik van die gegevens ten behoeve van een last onder dwangsom jegens dat ziekenhuis).
[67] EHRM 2 oktober 2014, AB 2015, 29, m.nt. T. Barkhuysen en M.L. van Emmerik (Delta Pekarny t. Tsjechie); zie eerder EHRM 14 maart 2013, nr. 24117/08, (Bernh Larsen Holding AS e.a. t. Noorwegen),

door middel van webcrawling in het algemeen wel eens een minder ruime beoordelingsmarge kunnen hebben dan bij andersoortige beperkingen het geval is.[68] De reden is dat het zich bij deze thematiek minder goed laat denken dat de lidstaten van de Raad van Europa sterk uiteenlopende visies hebben en dat het Hof niet de aangewezen instantie zou zijn om zijn om zich uit te laten over de noodzaak van de inbreuken.

2. Het gebruik van de techniek moet noodzakelijk zijn, gelet op de handhavingstaak van het betrokken bestuursorgaan. Dat betekent dat het in het belang moet zijn van een van de genoemde belangen in art. 8, tweede lid, EVRM. Het moet dus in het belang zijn van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Bij 1 en 2 speelt een rol in hoeverre is voorzien in een adequaat systeem van controle en rechtsbescherming om misbruik te voorkomen en in het bieden van gelegenheid te reageren de bevindingen. Het laat zich denken dat de betrokkene op een gegeven moment moet worden ingelicht over de via webcrawling verkregen informatie, voordat de via webcrawling verkregen informatie ten grondslag kan worden gelegd aan een besluit, in het bijzonder een bestuurlijke sanctie. Voorafgaand aan sanctie zal betrokkene moeten worden gehoord om en gelegenheid worden geboden om zijn visie te geven/corrigerende opmerkingen te maken. Echter, de staten zal ook daarbij in meer of mindere mate een margin of appreciation toekomen.[69]

3. Moet het gebruik van de methode zijn voorzien bij wet? Voldoende is volgens het EHRM dat er een wettelijke basis bestaat die de reikwijdte van een inmenging (of de bevoegdheid hiertoe) en de voorwaarden voor de uitoefening van de discretionaire bevoegdheid hiertoe bepaalt. De wet moet wel voldoende duidelijk geformuleerd zijn.[70] Er moet een bindende en toegankelijke regeling gelden; de gevolgen moeten voor de betrokkene zijn te voorzien en er moet geen risico zijn van willekeur in de toepassing.[71]
   Het problematische van webcrawling is dat een wettelijke regeling zich nog niet zo makkelijk laat denken. Wanneer in een concreet geval de vraag speelt of via webcrawling informatie mag worden verkregen die vervolgens mag worden gebruikt in het kader van bestuurlijke handhaving (in het bijzonder ter onderbouwing van een sanctiebesluit), is met name van belang of de resultaten die ermee zijn bereikt met zich brengen dat feitelijk een inbreuk op de persoonlijke levenssfeer van de betrokkene heeft plaatsgevonden. Het zal niet doenlijk zijn webcrawling te reguleren op basis van welke inbreuk op de privacy was te verwachten op het moment dat het instrument wordt ingezet. Dat maakt het moeilijk en wellicht ondoenlijk in wetgeving *in algemene zin* nauwkeurig te regelen onder welke omstandigheden bepaalde activiteiten die kwalificeren als webcrawling al dan niet toelaatbaar zijn.[72]
   Op zich is voor het voldoen een het criterium ‘bij wet voorzien’ geen wettelijke regeling vereist. De beperking moet accessible en foreseeable zijn. Ofwel: de inhoud van de betrokken regels moet

---

r.o. 159; EHRM 16 december 1992, Series A vol. 251–B, NJ 1993, 400, m.nt. Dommering (Niemetz), r.o. 31.

[68] Vgl. EHRM 11 december 2014, RAV 2015, 21 (Dubská and Krejzová v. the Czech Republic) (in Tsjechië is mogen verloskundigen slechts in een zorginstelling assistentie mogen verlenen.) Vgl. ook EHRM 20 mei 2014, NJB 2014, 1680: zeer ruime margin of appreciation bij vraagstukken van volksgezondheid en allocatie van publieke middelen. Belangenafweging op nationaal niveau.

[69] EHRM 20 december 2011, RvdW 2012/1221; EHRM 6 september 1978, app. no. 5029/71 (Klass e.a. t. Duitsland), par. 41-55; EHRM 26 maart 1987, app. no. 9248/81 (Leander t. Zweden), par. 48-59; T. Barkhuysen, ‘Het EVRM als integraal onderdeel van het Nederlandse materiële bestuursrecht’, in: De betekenis van het EVRM voor het materiële bestuursrecht (VAR-reeks 132), Den Haag: BJu 2004, p. 68.

[70] Vgl. ook EHRM 16 februari 2000, app. no. 27798/95, (Amman v. Switzerland), par. 44 en 62 .

[71] EHRM 25 september 2001, NJ 2003, 670, m.nt. EJD, EHRC 2001/76, m.nt. Spronken (P.G. en J.H. v. Verenigd Koninkrijk), r.o. 11-16.

[72] Vgl. hierover ook M.J. Borgers, ‘De normering van “lichte” opsporingshandelingen’, *DD* 2015/15, p. 143-155.

kenbaar zijn.[73] Beleidsregelgeving en vaste rechtspraak of zelfs een overheidspublicatie op het internet (!) kan volstaan. Echter, in het bijzonder wat gebruik gemaakt van instrumenten als webcrawling, zal net als bij gebruik van andere instrumenten waarvan het gebruik aan directe waarneming van betrokkenen is onttrokken, is een risico van willekeur. Dat vraagt in ieder geval om regels waarin grenzen worden gesteld aan het gebruik van het instrument die voldoende duidelijk zijn, specificeren wat de legitieme doelen zijn waarvoor het instrument mag worden ingezet en bescherming bieden tegen willekeurig gebruik. Daarbij behoort ook dat regels worden gesteld met betrekking tot de transparantie van de werkwijzen die worden gevolgd.[74] Zo laat zich denken dat steeds een logboek moet worden gemaakt van webcrawlingactiviteiten. De klager moet over de uitleg en toepassing van de betrokken regels kunnen procederen.'[75]

4.2.4 Art. 8 Handvest grondrechten Europese Unie

Artikel 8 Handvest grondrechten Europese Unie is een nieuw grondrecht in aanvulling op het bekende privacy grondrecht. Het vormt in wezen een nadere uitwerking de uitzondering op privacy zoals bijvoorbeeld te vinden in artikel 8 lid 2 EVRM. Een verwerking van persoonsgegevens maakt immers inherent een inbreuk op de persoonlijke levenssfeer, reden waarom in Nederland bijvoorbeeld in de Wbp waarborgen worden gesteld aan de verwerking. Dat is de "bij wet voorzien" van artikel 8 lid 2. Het grondrecht van gegevensverwerking vormt in wezen een herhaling van wat ten grondslag aan regelingen als de Wbp en Wpg ligt. Voor een beroep op het recht op bescherming van persoonsgegevens zoals neergelegd in artikel 8 van het Handvest is voldoende dat sprake is van de verwerking van gegevens die te herleiden zijn tot een te identificeren individu. Ingevolge artikel 8 lid 2 van het Handvest moeten persoonsgegevens eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Bovendien heeft eenieder recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan en ziet een onafhankelijke autoriteit toe op de naleving van deze regels.

4.2.5 Een wettelijke regeling voor gebruik van webcrawling in het kader van bestuurlijke handhaving

Gelet op het voorgaande en gelet op het criterium 'voor zover bij wet is voorzien' in art. 8 EVRM lijkt het aangewezen webcrawling van een wettelijke basis en normering te voorzien, ook al zullen de voorwaarden voor bevoegdheidsuitoefening niet in gesloten termen kunnen worden beschreven. Anders bestaat er bij gebruikmaking van gegevens die juist via webcrawling zijn verkregen, in gevallen waarin die gegevens de persoonlijke levenssfeer van betrokkene raken een serieus risico dat art. 8 EVRM geschonden is vanwege het ontbreken van een toereikende wettelijke basis.

De vervolgvraag is wat een goed aanknopingspunt voor een wettelijke regeling voor gebruik van webcrawling in het kader van handhaving door bestuursorganen zou kunnen zijn. Bij webcrawling wordt het internet doorzocht en daardoor kan in beginsel informatie over een ieder worden verzameld. Door het gebruik van specifieke methoden kan bij webcrawling echter meer specifieke informatie over een individu worden gekregen. De vraag of en wanneer die informatie die door de overheid is verkregen/gegenereerd zodanig is, dat het recht op bescherming van de persoonlijke levenssfeer (als bedoeld in artikel 8 EVRM) in het geding is, laat zich moeilijk in algemene zin beantwoorden. Dat maakt het moeilijk een algemene wettelijke regeling te maken.[76]

---

[73] EHRM 26 april 1979, NJ 1980, 146, m.nt. E.A. Alkema (Sunday Times), r.o. 49-53.

[74] EHRM 18 mei 2010, Kennedy v. VK, app.no. 26839/05, r.o. 152; EHRM 22 november 2012, Mediaforum 2013, 1, m.nt. W. Hins, NJ 2013/252, m.nt. E.J. Dommering, (Telegraaf v. the Netherlands) , r.o. 89-102. In het Telegraaf-arrest oordeelde het Hof dat de Nederlandse wetgeving geen passende waarborgen biedt met betrekking tot afluisterbevoegdheden die werden gebruikt jegens de twee Telegraaf-journalisten met het doel om hun journalistieke bronnen te achterhalen.

[75] EHRM 24 maart 1988, app.no. 10465/83 (Olson), r.o. 61-62.

[76] Vgl. in een andere context (grootschalige verzameling van telecommunicatiegegevens door de AIVD en de MIVD en buitenlandse inlichtingendiensten) Rb. Den Haag 23 juli 2014, *Computerrecht* 2014/186, m.nt. Rob van den Hoven van Genderen, r.o. 5.24.

Aangrijpingspunt voor wettelijke normering in de Awb zou kunnen/moeten zijn aan welke procedurele regels webcrawling gebonden is en onder welke condities de hiermee verkregen informatie aan een bestuurlijke sanctie ten grondslag mag liggen. Daartoe zou een proportionaliteitstoets (die aansluit bij de wijze waarop die door het Hof vorm is gegeven) in de wet, bijvoorbeeld de Awb, kunnen worden neergelegd. Tevens zouden enkele procedurele waarborgen in de Awb kunnen worden opgenomen, zoals een verplichting tot het loggen van de webcrawlingsactiviteiten, opdat navolgbaar is wat er is gedaan. Ook kan in de Awb worden bepaald dat via webcrawling verkregen gegevens slechts (mede) ten grondslag morgen liggen aan een handhavingsbesluit indien dat bij wet is voorzien.

Voor zover het gaat om wettelijke regelingen die in het belang zijn van één of meer van de in art. 8, tweede lid, genoemde doelen, zou daarin in de bevoegdheid tot webcrawling kunnen worden voorzien. Meer voor de hand ligt wellicht in meer algemene zin in de Awb een regeling op te nemen voor verkrijgen van informatie met andere middelen dan de in titel 5.2 Awb opgenomen toezichtsbevoegdheden. Voor zover het gaat om bestuurlijke bestraffende sanctie zou de regeling voor gebruik van via webcrawling verkregen gegevens strenger kunnen zijn en aangesloten kunnen worden bij het strafrecht. De algemene taakstellende bepalingen en/of bepalingen over stelselmatige inwinning of observatie in het strafrecht en de daarin opgenomen toepassingsvoorwaarden zouden daarbij tot voorbeeld kunnen strekken (zie strafrechtelijke hoofdstuk in dit rapport).

4.3 Conclusie

Informatie over de naleving van wettelijke voorschriften (in het kader van bestuursrechtelijke informatie) kan worden verkregen via uitoefening van de bevoegdheden die een toezichthouder op grond van de Awb of de bijzondere wet heeft, maar kunnen ook op andere wijze in beginsel worden gebruikt bij besluitvorming over oplegging van een bestuurlijke sanctie. Zo kan die informatie een startpunt zijn voor nader onderzoek waarbij door middel van webcrawling informatie over een persoon of bedrijf wordt blootgelegd, die met een gewone zoekopdracht op internet niet zou zijn verkregen en die van doorslaggevende betekenis kan zijn voor een bepaald besluit van een bestuursorgaan. Ook kunnen met de resultaten van webcrawling bij de uitoefening van toezichtsbevoegdheden als bedoeld in de Awb informatie worden verkregen over nalevingsgedrag. Webcrawling is geen toezichtshandeling waarop art. 5:13 Awb (een aanscherping van het evenredigheidsbeginsel van voor uitoefening van toezichtsbevoegheden als bedoeld in titel 5.2) van toepassing is, maar is wel feitelijk bestuurshandelen waarop onder meer de artikelen 3:2 tot en met 3:4 Awb van toepassing zijn. In het bijzonder het zorgvuldigheids- en het evenredigheidsbeginsel zijn van belang. Deze algemene beginselen van behoorlijk bestur zijn ingevolge art. 3:1, tweede lid, Awb op feitelijke handelingen van toepassing ‘voor zover de aard van de handelingen zich daartegen niet verzet’.

De eisen aan gebruik bij webcrawling zijn niet zo streng als die bij gebruik ervan in het kader van strafrechtelijke opsporing. Is met behulp van webcrawling informatie verkregen die strafrechtelijk als onrechtmatig verkregen bewijs kwalificeert dan zal gebruik ervan in het kader van bestuursrechtelijke besluitvorming, gelet op de jurisprudentie, niet toegestaan zijn indien het is verkregen op een wijze die zozeer indruist tegen die welke van een behoorlijk handelende overheid mag worden verwacht dat dit onder alle omstandigheden ontoelaatbaar moet worden geacht. Zeker mag aangenomen worden dat het gebruik ervan in het kader van bestuurlijk bestraffend optreden aan vergelijkbare beperkingen onderworpen is als gebruik ervan in het kader van strafrechtelijke opsporing.

Of webcrawling een inbreuk oplevert van het recht op bescherming van de persoonlijke levenssfeer als bedoeld in art. 8 EVRM hangt af van de aard van de verkregen informatie en of een min of meer compleet beeld ontstaat van bepaalde aspecten van het persoonlijk leven van een persoon. Voor de beantwoording van de vraag of een dergelijke inbreuk vervolgens ook geoorloofd is, zijn de criteria van art. 8, tweede lid, EVRM bepalend. Het gebruik van webcrawling moet in het belang zijn van één van de in dat artikellid genoemde belangen. De persoonlijke levenssfeer van de betrokkene mag daarbij niet onevenredig worden geschaad. Er moet bij webcrawling een adequate rechterlijke toetsing

op dit aspect plaats kunnen vinden. De verdragsstaten komt een beoordelingsmarge toe bij beoordeling van de evenredigheid van een inbreuk, maar die zou wel eens beperkt kunnen zijn gelet op de kwestie waar het om gaat. Het is goed verdedigbaar dat via webcrawling verkregen informatie in beginsel eerst moet worden voorgelegd aan betrokkene, voordat zij ten grondslag kan worden gelegd aan een ingrijpend besluit.

Ingevolge art. 8, tweede lid, EVRM is een inmenging in het recht op bescherming van de persoonlijke levenssfeer alleen toelaatbaar 'voor zover bij wet is voorzien'. Een wettelijke regeling die specifiek ziet op het gebruik van webcrawling is er niet. Belangrijk is dat er gelet op de jurisprudentie overheidsdocumentatie lijkt te moeten zijn op basis waarvan kenbaar en voorzienbaar is onder welke condities gebruik van een instrument als dit geoorloofd. Dit kan ook beleidsregelgeving, vaste rechtspraak of een internetpublicatie van de overheid zijn. Het is op dit moment niet duidelijk welke eisen er gelet op art. 8, tweede lid, EVRM zouden gelden met betrekking tot status en inhoud van regels voor gebruik van webcrawling. Er behoort voldoende transparantie met betrekking tot het gebruik van dit instrument te worden gegarandeerd en er moet gelegenheid voor betrokkene zijn om zijn zienswijze te geven op de verkregen informatie. Er moet in ieder geval bescherming bij de rechter mogelijk zijn tegen willekeurig gebruik. Betrokkene moeten dus kunnen procederen over de wijze waarop het instrument is gebruikt of de inhoud van de verkregen informatie.

De vraag is wat de aanknopingspunten zijn voor een adequate (wettelijke) regeling die voldoet aan de direct werkende mensenrechtenbepalingen. De bevoegdheden tot webcrawling en andere instrumenten dan die welke thans genoemd zijn in titel 5.2 Awb moeten, als zij resulteren in een inbreuk op iemands persoonlijke levenssfeer, alleen aangewend (kunnen) worden als dat dat een belang dient als bedoeld in art. 8, tweede lid, EVRM. In de Awb zouden regels opgenomen kunnen worden over het gebruik van andere instrumenten dan de in titel 5.2 genoemde bevoegdheden. Hierbij kan inspiratie worden gevonden bij de algemene taakstellende bepalingen en/of bepalingen over stelselmatige inwinning of observatie in het strafrecht en de daarin opgenomen toepassingsvoorwaarden uit het strafrecht (Sv. en Politiewet).

Verder zou de Awb in het algemeen voor gebruik van andere methoden van informatieverwerving dan die via de uitoefening van de toezichtbevoegdheden als bedoeld in titel 5.2 Awb (zoals webcrawling) moeten voorzien zijn in een proportionaliteitstoets met betrekking tot de inzet van een instrument en in regels over transparantie en de mogelijkheid van een weerwoord voor betrokkene, ongeacht het soort besluit waarvoor de verkregen informatie wordt gebruikt.

5 Strafrechtelijke opsporing

5.1 Inleiding

Dit hoofdstuk handelt over de vraag of de *verkrijging* van gegevens door middel van webcrawling op grond van de huidige strafvorderlijke wetgeving toelaatbaar is. Daartoe moet als uitgangspunt worden genomen dat strafvervolging alleen geschiedt op de wijze bij de wet voorzien (artikel 1 Sv). Deze strafvervolging vangt aan met het opsporingsonderzoek.[77] Onder opsporing wordt verstaan, aldus artikel 132a Sv, het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen. Het gaat hier om een ruim opsporingsbegrip, in die zin dat van opsporing reeds sprake kan zijn voordat een verdachte in beeld komt en ook voordat strafbare feiten zijn gepleegd.[78] Wanneer er door opsporingsinstanties informatie wordt verzameld (en opgeslagen) met als doel om daar – al dan niet na bewerking van die informatie – op een later moment gebruik van te (kunnen) maken in verband met het onderzoek naar strafbare feiten, kan die activiteit reeds als opsporing worden aangemerkt. Willen de resultaten van webcrawling kunnen worden gebruikt in strafzaken, dan zal moeten komen vast te staan dat er een toereikende wettelijke grondslag voorhanden is. Ontbreekt die grondslag, dan geldt dat het verkrijgen van gegevens door middel van webcrawling een vormverzuim oplevert, waaraan op de voet van artikel 359a Sv rechtsgevolgen kunnen worden verbonden. Ook moet erop worden gewezen dat verwerking van politiegegevens alleen is toegestaan wanneer die gegevens rechtmatig zijn verkregen (artikel 3 lid 2 Wpg).

Het Wetboek van Strafvordering kent geen regeling die specifiek is toegesneden op het verkrijgen van informatie door middel van webcrawlers. Ook de bijzondere wetgeving – zoals de WWM – voorziet daar niet in. Daarmee is echter nog niet gezegd dat webcrawling onrechtmatig moet worden geacht. Dat opsporingsmethoden gelet op artikel 1 Sv een wettelijke grondslag vergen, betekent niet dat telkens een specifieke – dat wil zeggen: specifiek op de desbetreffende opsporingsmethode toegesneden – wettelijke regeling moet bestaan. Het is vaste rechtspraak dat algemene taakstellende bepalingen als toereikende wettelijke grondslag kunnen dienen voor – wat men zou kunnen noemen – 'lichte' opsporingshandelingen (of opsporingsmethoden). Die bepalingen betreffen artikel 3 Politiewet 2012 en artikel 141/142 Sv.[79] Op grond van deze artikelen is een opsporingsambtenaar bevoegd, zo oordeelt de Hoge Raad, om een niet specifiek in de wet geregelde wijze van opsporing in te zetten op een wijze die een beperkte inbreuk maakt op grondrechten van burgers en die niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing.[80] Voorts is het mogelijk om te onderzoeken of (bepaalde vormen van) de inzet van webcrawlers valt te scharen onder reeds bestaande, specifiek in de wet geregelde opsporingsbevoegdheden, ook al zijn die bevoegdheden oorspronkelijk niet in het leven geroepen met het oog op webcrawling. Daarbij kan in het bijzonder worden gedacht aan de bijzondere opsporingsbevoegdheden stelselmatige observatie en stelselmatige inwinning van informatie. In het verlengde hiervan kan worden gewezen op de mogelijkheden die de wet biedt voor het verkennend onderzoek.

In het navolgende zal allereerst worden onderzocht of, en zo ja: in hoeverre, de algemeen taakstellende bepalingen een toereikende grondslag bieden, en vervolgens of webcrawling zou kunnen plaatsvinden op grond van de bevoegdheden tot stelselmatige observatie en/of stelselmatige inwinning van informatie dan wel in het kader van het verkennend onderzoek. In zekere zin is deze volgorde

[77] Zie daarover J.M. Reijntjes, Boef of burger?, Arnhem: Gouda Quint 1989, p. 4. Vgl. ook HR 12 april 1897, W. 1897, 6964.

[78] Zie voor een meer uitvoerige beschouwing omtrent het opsporingsbegrip van artikel 132a Sv, met nadere verwijzingen, G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers, Deventer: Kluwer 2014, p. 281-289.

[79] Zie daarover B.F. Keulen & G. Knigge, *Strafprocesrecht*, Deventer: Kluwer 2010, p. 283-286 en Corstens/Borgers 2014, p. 25-26. Vgl. voorts J.W. Fokkens & N. Kirkels-Vrijman, 'De artikelen 2 Politiewet 1993 en 141 en 142 Sv als basis voor opsporingsbevoegdheden', in: M.J. Borgers e.a. (red.), *Politie in beeld*, Nijmegen: Wolf Legal Publishers 2009, p. 105-124.

[80] Zie bijvoorbeeld HR 1 juli 2014, ECLI:NL:HR:2014:1562.

willekeurig: wanneer geconstateerd wordt dat de algemeen taakstellende bevoegdheden een toereikende wettelijke grondslag bieden, is het strikt genomen niet nodig om naar de specifieke wettelijke bevoegdheden te kijken. Dat geldt ook vice versa: wanneer een opsporingshandeling kan worden gebaseerd op een specifieke wettelijke bevoegdheid, dan ontbreekt de noodzaak om te onderzoeken of de algemene taakstellende bepalingen als grondslag kunnen worden aangewezen. Het zal evenwel blijken dat aan alle genoemde mogelijke grondslagen haken en ogen kleven, zodat het zinvol is om op elk daarvan in te gaan. De volgorde waarin dat geschiedt, is dan niet van groot belang.

5.2 Algemene taakstellende bepalingen

De algemene taakstellende bepalingen bieden een toereikende wettelijke grondslag voor 'lichte' opsporingshandelingen. Zoals hiervoor is weergegeven verschaffen deze bepalingen de bevoegdheid om een niet specifiek in de wet geregelde wijze van opsporing in te zetten op een wijze die een beperkte inbreuk maakt op grondrechten van burgers en die niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing. Artikel 3 Politiewet 2012 en artikel 141/142 Sv bakenen daarmee niet heel nauwkeurig het speelveld voor de opsporingsambtenaar af. Eerst wanneer wordt vastgesteld dat een opsporingshandeling a) een meer dan beperkte inbreuk maakt op grondrechten, dan wel b) zeer risicovol is voor de integriteit en beheersbaarheid,[81] moet die opsporingshandeling achterwege blijven (althans geldt dat die opsporingshandeling alleen mag worden verricht indien daartoe een specifieke wettelijke bevoegdheid bestaat). Aldus wordt een tweetal gezichtspunten aangereikt aan de hand waarvan vooraf kan worden bepaald of op grond van de algemene taakstellende bepalingen een bepaalde opsporingshandeling mag worden verricht, dan wel achteraf kan worden nagegaan of het verrichten daarvan rechtmatig is geweest.[82] Onderzocht kan derhalve worden of, en zo ja: in hoeverre, het gebruik van webcrawlers is toegestaan op grond van die taakstellende bepalingen.

Er bestaat geen aanleiding om aan te nemen dat aan de inzet van webcrawlers grote risico's voor de integriteit en beheersbaarheid van de opsporing zijn verbonden.[83] Waar zich risico's voordoen, houden die veeleer verband met de schending van fundamentele rechten van burgers, in het bijzonder de bescherming van de persoonlijke levenssfeer.[84] Centraal staat dus de vraag of het vergaren van gegevens door middel van webcrawling een beperkte dan wel een meer dan beperkte inbreuk maakt op de privacy. In de rechtspraak van de Hoge Raad wordt tot uitgangspunt genomen dat er sprake is van een meer dan beperkte inbreuk op de privacy wanneer een opsporingshandeling in verband met de duur, intensiteit en frequentie ervan, alsmede het gebruik van technische hulpmiddelen, geschikt is om een min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijk leven van de betrokkene.[85] In de rechtspraak van de Hoge Raad wordt dit uitgangspunt niet alleen betrokken op observaties van een verdachte, maar ook op andere opsporingsmiddelen, zoals het bepalen van een locatie door middel van een stille sms of de inzet van een IMSI-catcher met het oog op locatiebepaling.[86]

Alvorens de inzet van webcrawlers te toetsen aan het door de Hoge Raad geformuleerde uitgangspunten dienen twee opmerkingen te worden gemaakt. Allereerst kan erop worden gewezen

[81] Het gaat erom of er geen wegen worden ingeslagen waarbij zaken uit de hand kunnen lopen. Denk aan het runnen van informanten in de IRT-affaire, dat ertoe leiden dat onder toeziend oog van de politie er containers drugs het land binnenkwamen.

[82] Een overzicht van de opsporingshandelingen die in de rechtspraak toelaatbaar worden geacht op grond van artikel 3 Politiewet 2012 en artikel 141/142 Sv, treft men aan bij J. Naeyé, *De organisatie van de Nationale Politie*, Deventer: Kluwer 2014, p. 140-150.

[83] In de rechtspraak is niet nader uitgewerkt wanneer dergelijke risico's zich (kunnen) voordoen. Gedacht lijkt te moeten worden aan opsporingsmethoden waarbij opsporingsambtenaren zelf betrokken raken bij de uitvoering van strafbare feiten en aan opsporingsmethoden waarbij het notoir lastig is om toezicht te houden op de wijze van uitvoering van die methoden.

[84] Zie over de betekenis van artikel 8 EVRM voor webcrawling hoofdstuk 4 van dit rapport.

[85] Zie bijvoorbeeld HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013/413 m.nt. M.J. Borgers.

[86] HR 1 juli 2014, ECLI:NL:2014:1563, *NJ* 2015, 114 en HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015, 115 m.nt. P.H.P.H.M.C. van Kempen.

dat de Hoge Raad spreekt van een min of meer compleet beeld van *bepaalde aspecten* van het persoonlijk leven van de betrokkene. Aangenomen mag worden – nu het hier gaat om de bescherming van de persoonlijke levenssfeer – dat die aspecten van dien aard moeten zijn dat deze ook echt raken aan een zekere sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen.[87] Van een meer dan beperkte inbreuk op het recht op bescherming van de persoonlijke levenssfeer lijkt derhalve niet snel sprake te zijn. De tweede opmerking betreft de wijze van toetsing: deze is niet (zozeer) prospectief, maar (veeleer) retrospectief van aard. Wanneer in een concreet geval de vraag speelt of een bepaalde opsporingshandeling op grond van de algemene taakstellende bepalingen mocht worden uitgevoerd, wordt vooral gekeken naar de resultaten die met die opsporingshandeling zijn bereikt en daarmee naar de inbreuk op de persoonlijke levenssfeer van de verdachte die feitelijk heeft plaatsgevonden. Het gaat niet, althans niet primair, om de vraag welke inbreuk op de privacy was te verwachten op het moment dat de opsporingshandeling werd ingezet.[88] Consequentie hiervan is dat het lastig is om *in algemene zin* uitspraken te doen over de toelaatbaarheid van opsporingshandelingen op grond van de algemene taakstellende bepalingen.[89] Op de keper beschouwd wordt immers van het resultaat – de daadwerkelijke privacy-inbreuk – terug geredeneerd naar de toelaatbaarheid van het middel waarmee dat resultaat is bereikt. Tegen deze achtergrond lijkt het vooral zinvol om na te gaan hoe groot de inbreuk op de persoonlijke levenssfeer in potentie kan zijn door de inzet van webcrawlers.

Bij webcrawling gaat het om het verzamelen en opslaan van informatie die op zich vrij beschikbaar is op het internet. Bij wijze van spreken betreft het informatie die elke willekeurige internetgebruiker zou kunnen opzoeken en – desgewenst – ook vastleggen. Niet gezegd is dat de informatie die wordt aangetroffen, telkens privacygevoelig van aard is, dat wil zeggen een min of meer compleet beeld schept van bepaalde aspecten van het persoonlijk leven van een bepaalde persoon. Voor zover dat wel het geval is, is daarmee niet gezegd dat ook een inbreuk op het recht op de persoonlijke levenssfeer is gemaakt. Niet uitgesloten is immers is dat de persoon in kwestie zelf de desbetreffende informatie op internet beschikbaar heeft gemaakt (bijvoorbeeld door die informatie te verschaffen in een weblog). Maar ook indien privacygevoelige informatie buiten de persoon die de informatie betreft om op internet is geplaatst, lijkt bezwaarlijk te kunnen worden gezegd dat de persoon die deze informatie op internet aantreft, reeds door het raadplegen van die informatie een inbreuk maakt op de persoonlijke levenssfeer. Die inbreuk is dan primair toe te rekenen aan degene die de informatie openbaar heeft gemaakt.

Wat webcrawling evenwel anders maakt dan het opzoeken en vastleggen van informatie door een willekeurig persoon, is dat webcrawling geautomatiseerd verloopt,[90] waardoor er veel meer informatie kan worden gevonden en vastgelegd. Vervolgens kan door indexering en bewerking van de verkregen en vastgelegde gegevens informatie worden afgeleid die niet of niet snel kenbaar zou zijn voor een willekeurige internetgebruiker. Het systematisch en geautomatiseerd opzoeken, vastleggen en gericht bewerken van op internet beschikbare gegevens is derhalve een activiteit die niet op één lijn kan worden gesteld met het 'gewoon' opzoeken van informatie door een individuele internetgebruiker.[91]

[87] Zie hieromtrent de noot onder HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013/413.

[88] Ter volledigheid: bij de afweging of stelselmatige observatie als opsporingsbevoegdheid zal moeten worden ingezet, is wel de verwachting leidend in welke mate een inbreuk op de privacy zal worden gemaakt. Wanneer echter zonder een bevel tot stelselmatige observatie wordt gehandeld en nadien wordt betoogd dat een meer dan geringe inbreuk is gemaakt op de privacy, gaat in de rechtspraak de aandacht uit naar de inbreuk die feitelijk is gemaakt en niet, althans niet specifiek, naar de inbreuk die tevoren viel te verwachten.

[89] Vgl. hierover ook M.J. Borgers, 'De normering van "lichte" opsporingshandelingen', *DD* 2015/15, p. 143-155.

[90] Dat er een technisch hulpmiddel wordt ingezet, duidt er reeds op dat er sprake is van een stelselmatige en (dus) niet-geringe inbreuk op de privacy. Vgl. Kamerstukken II 1996/1997, 25 403, nr. 3, p. 110.

[91] In Kamerstukken II 1989/99, 26 671, nr. 3, p. 35 wordt opgemerkt dat de politie op grond van de algemeen taakstellende bepalingen bevoegd is om rond te kijken op internet. Echter, van gewoon rondkijken is bij webcrawling geen sprake. Om die reden heeft deze opmerking weinig betekenis, te meer wanneer men bedenkt dat die meer dan vijftien jaar geleden is gemaakt. Te wijzen valt ook op de volgende opmerking in Kamerstukken II 1989/99, 26 671, nr. 3, p. 36: 'De bevoegdheid om rond te kijken op een openbaar netwerk

Hier spelen derhalve de eerder genoemde gezichtspunten van de duur, intensiteit en frequentie ervan, alsmede het gebruik van technische hulpmiddelen, een rol. Bij webcrawling wordt gedurende langere tijd (en dus herhaaldelijk) intensief gezocht naar mogelijk relevante gegevens, daarbij gebruik makend van technische hulpmiddelen voor het opzoeken en vastleggen van die gegevens. Juist daardoor bestaat de mogelijkheid dat een min of meer compleet beeld ontstaat van bepaalde aspecten van het persoonlijke leven van een persoon.[92] Let wel: het gaat om de mogelijkheid. Immers, het zal afhangen van de informatie die wordt aangetroffen,[93] of er een dergelijk beeld ontstaan. En zo dat het geval is, of de aspecten van het persoonlijke leven ook raken aan een zekere sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen.

Van belang is ook dat er geen alomvattende regeling bestaat met betrekking tot de toegang en het gebruik van gegevens die door middel van webcrawling zijn verzameld. De verwerking van persoonsgegevens wordt, voor zover het gaat om de verwerking binnen de politieorganisatie, genormeerd door de Wet politiegegevens. Er zijn geen voorschriften die specifiek zien op het opvragen en gebruiken van door middel van webcrawling vastgelegde gegevens. Hierdoor ontbreken ook bepalingen waaruit zekere beperkingen voortvloeien ter zake van de omstandigheden waaronder dergelijke gegevens mogen worden opgevraagd en gebruikt, of met betrekking tot de daartoe bevoegde autoriteiten.[94] Mede in het licht van de rechtspraak van het EHRM en het HvJ EU is het ontbreken van een dergelijke normering een relevante omstandigheid bij de vaststelling van een inbreuk op de privacy.

Vastgesteld lijkt te mogen worden dat webcrawling heel wel een meer dan beperkte inbreuk kan maken op de privacy van een persoon. Die inbreuk wordt niet veroorzaakt doordat gevoelige informatie omtrent een persoon openbaar wordt gemaakt door plaatsing van die informatie op internet, maar doordat er (van overheidswege) systematisch en geautomatiseerd gegevens worden verzameld, waarbij die gegevens – al dan niet na bewerking daarvan – informatie omtrent een persoon blootleggen. Het is dan afhankelijk van de aard van de informatie die wordt verkregen, of een min of meer compleet beeld ontstaat van bepaalde – aan een zekere sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen rakende – aspecten van het persoonlijke leven van een persoon.
Bij deze stand van zaken vormen de algemeen taakstellende bepalingen hooguit een onzekere grondslag voor webcrawling. De situatie kan zich voordoen dat uit de gegevens die met webcrawling worden verkregen, wel bruikbare, maar geen privacygevoelige informatie omtrent een verdachte naar voren komt.[95] In dat geval zal een verweer van de verdachte van de strekking dat een toereikende wettelijke grondslag heeft ontbroken, waarschijnlijk falen.[96] Echter, wanneer er wel informatie is verkregen van dien aard dat een min of meer compleet beeld ontstaat van bepaalde – aan een zekere

---

impliceert nog niet de bevoegdheid om stelselmatig voor de uitoefening van de politietaak gegevens omtrent onverdachte personen van Internet te downloaden en in een politieregister op te slaan.' (Overigens wordt in deze passage vooral acht geslagen op de mogelijkheden die de toenmalige Wet politieregisters bood voor de opslag van gegevens. Het accent ligt niet op de bevoegdheid tot verkrijging van de gegevens.)

[92] Zie ook, met nadere verwijzingen naar rechtspraak van het EHRM, B.J. Koops, 'Politieonderzoek in open bronnen op internet, Tijdschrift voor Veiligheid 2012, p. 34-37 en J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', Justitiële Verkenningen 2012, nr. 5, p. 40-42, 45-46.

[93] En nog een stap daarvoor: van de informatie die op enigerlei wijze beschikbaar is op het internet. Wat niet beschikbaar is, kan immers ook niet worden aangetroffen.

[94] Overigens wordt in de rechtspraak wel betekenis toegekend aan de omstandigheid dat, ook al is dat niet voorgeschreven, wel zekere beperkingen in acht zijn genomen bij het ontplooien van opsporingshandelingen. Zo wordt in de rechtspraak het feit dat de officier van justitie toestemming heeft gegeven, veelal betrokken als relevant gegeven bij het aanvaarden van de algemene taakstellende bepalingen als toereikende wettelijke grondslag. Echter, uit deze rechtspraak laat zich niet goed afleiden wanneer een buitenwettelijke normering toereikend is om betrekkelijk zware inbreuken op fundamentele rechten gerechtvaardigd te achten, wanneer daarvoor geen specifieke wettelijke grondslag bestaat. Zie hierover nader Borgers 2015.

[95] Vgl. ook, al gaat het daarbij niet specifiek om webcrawling, W.Ph. Stol, E.R. Leukfeldt en H. Klap, 'Cybercrime en politie', *Justitiële Verkenningen* 2012, nr. 1, p. 30.

[96] Het gaat immers niet om de potentiële inbreuk die een bepaald opsporingsmiddel kan maken, maar om de inbreuk die daadwerkelijk in de concrete zaak jegens de verdachte is gemaakt.

sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen rakende – aspecten van het persoonlijke leven van de verdachte, zal eenzelfde verweer wel slagen. Vanuit het oogpunt van effectieve rechtshandhaving is het een weinig aanlokkelijke situatie wanneer het mede afhankelijk is van de resultaten die met webcrawling worden geboekt, of webcrawling als opsporingsmethode al dan niet als rechtmatig heeft te gelden.

5.3 Stelselmatige observatie en stelselmatige inwinning van informatie

Nu webcrawling in beginsel een meer dan beperkte inbreuk maakt op de persoonlijke levenssfeer, rijst de vraag of webcrawling zou kunnen plaatsvinden op basis van specifieke wettelijke grondslagen voor opsporingsmethoden. Gedacht moet dan worden aan zowel stelselmatige observatie als stelselmatige inwinning van informatie,[97] nu webcrawling trekken heeft van zowel observatie als het inwinnen van informatie. Van observatie is in zoverre sprake dat er wordt rondgekeken op internet, teneinde waar te nemen of daarop relevante informatie is te vinden omtrent de gedragingen van een persoon. Deze activiteit zou men ook kunnen aanmerken als het inwinnen, want verzamelen, van informatie omtrent een persoon.

Tegelijkertijd sluit webcrawling niet naadloos aan bij de opsporingsmethode die de wetgever voor ogen had bij het opstellen van de wettelijke voorschriften ter zake van stelselmatige observatie en stelselmatige inwinning van informatie. Bij een reguliere observatie worden gedragingen waargenomen op het moment dat die gedragingen worden gesteld. Het gaat daarbij om de gedragingen van de te observeren persoon zelf. De wet spreekt hier van het volgen van een persoon of het waarnemen van diens aanwezigheid of gedrag. Bij webcrawling wordt echter niet in letterlijke zin een persoon gevolgd of diens aanwezigheid of gedrag waargenomen. Veeleer wordt informatie verzameld waaruit een en ander kan worden afgeleid over activiteiten van een persoon. Het gaat daarbij in zekere zin om historische informatie. Bij webcrawling wordt immers gezocht naar informatie die reeds beschikbaar is gesteld op het internet. Zo bezien, heeft webcrawling ogenschijnlijk meer trekken van het stelselmatig inwinnen van informatie. Bij de wettelijke regeling van die bevoegdheid lijkt echter vooral te zijn gedacht aan het door een opsporingsambtenaar actief benaderen van personen om informatie in te winnen over een (toekomstige) verdachte, zonder dat die ambtenaar daarbij kenbaar maakt in welke hoedanigheid hij dat doet.[98] Bij webcrawling is er niet in deze zin sprake van het actief interfereren in het leven van de (toekomstige) verdachte. Veeleer gaat het om het verzamelen van informatie die reeds beschikbaar is, zonder dat de persoon die voorwerp is van onderzoek, zelf of diens directe omgeving behoeft te worden benaderd.[99] Wel is er in zoverre een overeenkomst dat ook bij webcrawling, door afscherming van het IP-adres, niet kenbaar wordt gemaakt dat door de politie informatie wordt gezocht.[100]

Het lijkt dus lastig om in stelselmatige observatie dan wel stelselmatige inwinning van informatie een eenduidige grondslag voor webcrawling te vinden.[101] Echter, betoogd zou kunnen worden dat webcrawling heel dicht aan ligt tegen beide opsporingsmethoden. Betoogd zou dan kunnen worden dat webcrawling als een toelaatbare opsporingsmethode moet worden opgevat, mits er aansluiting wordt gezocht bij de voorwaarden die de wet stelt aan stelselmatige observatie en stelselmatige inwinning van informatie. Relevant daarbij is dat de toepassingsvoorwaarden voor beide

[97] Zie artikel 126g, 126o en 126zd Sv respectievelijk artikel 126j, 126qa en 126zd Sv.
[98] Vgl. Kamerstukken II 1996/97, 25 403, nr. 3, p. 34. Als voorbeeld wordt hier genoemd het deelnemen aan een newsgroup op internet door een opsporingsambtenaar.
[99] Vgl. ook Koops 2012, p. 38.
[100] Er wordt daardoor informatie vergaard zonder dat kenbaar wordt gemaakt wie die informatie verlangd. Het is echter de vraag of bij webcrawling in dezelfde mate van als bij het stelselmatig inwinnen van informatie 'in levende lijve' sprake is van misleiding de opsporingsambtenaar zijn hoedanigheid niet bekend maakt. Bij webcrawling wordt IP-informatie afgeschermd, maar behoeft geen bepaald beeld te worden geschetst tegenover een bron om informatie los te krijgen. Vgl. hierover Koops 2012, p. 38-40.
[101] Om die reden pleiten J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', Justitiële Verkenningen 2012, nr. 5, p. 46-47 voor een afzonderlijke wettelijke regeling voor observatie in een internetomgeving.

bevoegdheden heel nauw op elkaar aansluiten. Dat levert een argument op voor de stelling dat het eigenlijk niet zoveel uitmaakt of webcrawling zou moeten worden gezien als observatie dan wel juist als inwinning van informatie.

Er is geen rechtspraak voorhanden dat met de zojuist geschetste extensieve uitleg van de wettelijke voorschriften ter zake van stelselmatige observatie en stelselmatige inwinning van informatie een specifieke wettelijke grondslag kan worden gecreëerd. Ervan uitgaande dat deze uitleg zou worden aanvaard, geldt echter niet dat webcrawling zonder meer is toegestaan. Er zou dan immers moeten worden voldaan aan de voorwaarden die de wet stelt aan stelselmatige observatie en stelselmatige inwinning van informatie. Conform de systematiek van de wetgeving ter zake van bijzonder opsporingsbevoegdheden dient er – naast andere voorwaarden – sprake te zijn van a) een verdenking ter zake van een misdrijf, b) een redelijk vermoeden ter zake van het in georganiseerd verband plegen of beramen van misdrijven als omschreven in artikel 67 lid 1 Sv, die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, dan wel c) aanwijzingen van een terroristisch misdrijf. In deze toepassingsvoorwaarde schuilt een belangrijke beperking in relatie tot webcrawling. Immers, het inzetten van webcrawling in de situatie dat nog geen concreet strafbaar feit in beeld is, is op de hier besproken grondslag niet mogelijk.

In relatie tot stelselmatige observatie bepaalt de wet dat de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel wordt aangewend, voor zover daarmee geen vertrouwelijke communicatie wordt opgenomen (artikel 126g lid 3 Sv). Op grond van artikel 126ee Sv worden bij algemene maatregel van bestuur – het Besluit technische hulpmiddelen strafvordering – allerhande voorschriften gesteld aan de inzet van dergelijke hulpmiddelen. Dat betekent dat, wanneer men webcrawling hanteert als vorm van stelselmatige observatie, de apparatuur waarmee deze webcrawling plaatsvindt, moet voldoen aan de technische eisen en keuringsvoorschriften die in het genoemde besluit worden gesteld. Het voert te ver deze voorschriften hier nader te bespreken. Opgemerkt kan wel worden dat die voorschriften niet specifiek zijn toegesneden op webcrawling. Ter volledigheid moet nog worden vermeld dat de notificatieverplichting van toepassing is wanneer toepassing wordt gegeven aan de bevoegdheden tot stelselmatige observatie en stelselmatige inwinning van informatie (artikel 126bb lid 1 Sv). Wanneer webcrawling zou plaatsvinden op grond van één van deze bevoegdheden of een combinatie daarvan, zou die notificatieverplichting – vanwege de grote schaal waarop informatie wordt ingewonnen – een grote administratieve last kunnen opleveren.[102] Ook kan worden genoemd dat ten aanzien van beide bevoegdheden diverse beleidsregels (met name de Aanwijzing opsporingsbevoegdheden) gelden, maar dat deze niet zijn toegesneden op het inzetten van stelselmatige observatie of stelselmatige informatie-inwinning in de vorm van webcrawling.

5.4 Verkennend onderzoek

Het Wetboek van Strafvordering bevat een regeling voor een zogeheten verkennend onderzoek. Indien uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in artikel 67 lid 1 Sv, die gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, kan de officier van justitie bevelen dat opsporingsambtenaren daarnaar een onderzoek instellen (artikel 126gg lid 1 Sv). Het doel van dit onderzoek is gelegen in, zo stelt de wet, de voorbereiding van de opsporing. Daarmee wordt – op enigszins ongelukkige wijze[103] – tot uitdrukking gebracht dat het verkennend onderzoek reeds mag worden verricht voordat er sprake is van een verdenking ter zake van een misdrijf of een redelijk

[102] Wetsvoorstel 33 747 brengt hierin ook geen wijziging. Zie voor een korte bespreking van dat wetsvoorstel Corstens/Borgers 2014, p. 594.
[103] Gelet op artikel 132a Sv geldt hetgeen hier als voorbereiding van opsporing wordt aangemerkt, reeds als opsporing. Aan deze terminologische kwestie behoeft hier echter geen aandacht te worden besteed. Zie nader Corstens/Borgers 2014, p. 285-286.

vermoeden ter zake van – kort gezegd – het in georganiseerd verband plegen of beramen van misdrijven. De wet stelt buiten twijfel dat reeds dan informatie mag worden verzameld, bewerkt, gebruikt en geanalyseerd door opsporingsambtenaren. Echter, er worden in relatie tot het verkennend onderzoek geen afzonderlijke bevoegdheden ter zake van de wijze van informatievergaring verstrekt. Het verkennend onderzoek vindt plaats, aldus de memorie van toelichting, op basis van informatie uit open bronnen[104] en informatie die vrijwillig door particulieren wordt verstrekt.[105] Voor wat betreft de informatie uit open bronnen lijkt daarbij niet te zijn gedacht aan complexe wijzen van het verkrijgen van informatie uit internetbronnen zoals webcrawling. Veeleer lijkt uit de verwijzing naar informatie uit open bronnen – juist ook omdat de regeling van het verkennend onderzoek niet (specifiek) is toegesneden op de wijze van verzameling van informatie – te moeten worden afgeleid dat het gaat om informatie die kan worden verzameld zonder dat daartoe een specifieke wettelijke grondslag noodzakelijk is. Anders gezegd: het verzamelen van informatie ten behoeve van een verkennend onderzoek dient plaats te vinden op grond van de algemene taakstellende bepalingen, althans dat verzamelen kan niet verder strekken dan waartoe die algemene taakstellende bepalingen legitimeren.[106] In relatie tot webcrawling geldt daarmee dat binnen het verkennend onderzoek dezelfde begrenzingen van kracht zijn als reeds hiervoor in relatie tot de algemene taakstellende bepalingen zijn besproken.
De mogelijkheden om verkennend onderzoek te verrichten zijn wel ruimer indien dat onderzoek betrekking heeft op (de voorbereiding van) de opsporing van terroristische misdrijven. Alsdan zijn er bevoegdheden die betrekking hebben op het verstrekken van geautomatiseerde gegevensbestanden (artikel 126hh Sv) en het opvragen van identificerende gegevens van personen en van gegevens van telecommunicatiegebruikers (artikel 126ii Sv). Voor de mogelijkheden van webcrawling zijn deze bevoegdheden echter niet van bijzonder belang.

5.5 Conclusie

Vastgesteld kan worden dat webcrawling zich niet eenvoudig laat inpassen in de wettelijke regeling van opsporingsbevoegdheden. Tot op zekere hoogte kan een grondslag worden gevonden in de algemene taakstellende bepalingen. Echter wanneer er informatie is verkregen van dien aard dat een min of meer compleet beeld ontstaat van bepaalde – aan een zekere sfeer van vertrouwelijkheid, intimiteit of het zich onopgemerkt mogen wanen rakende – aspecten van het persoonlijke leven van de verdachte, bieden die bepalingen geen toereikende grondslag. Geconstateerd is reeds dat het vanuit het oogpunt van effectieve rechtshandhaving een weinig aanlokkelijke situatie is om de rechtmatigheid van webcrawling als opsporingsmethode mede afhankelijk te laten zijn van de resultaten die met webcrawling worden geboekt.

Webcrawling laat zich ook niet goed in passen in de specifiek wettelijk geregelde opsporingsbevoegdheden. Een grondslag kan nog het beste worden gevonden in een combinatie van de bevoegdheden tot stelselmatige observatie en stelselmatige inwinning van informatie. Maar er is geen rechtspraak waarin uitsluitsel wordt gegeven omtrent de geldigheid van zo'n gecombineerde grondslag. Daarbij komt dat er, als men die geldigheid wel aanneemt, zodanige toepassingsvoorwaarden gelden dat webcrawling niet ongelimiteerd kan worden ingezet.

Het is niet uitgesloten dat webcrawling een onderdeel kan zijn van een verkennend onderzoek, maar hier geldt de beperking dat de regeling van het verkennend onderzoek geen bevoegdheden biedt tot

[104] Zie nader over het begrip 'open bronnen' Koops 2012, p. 33.
[105] Kamerstukken II 1996/97, 25 403, nr. 3, p. 49. Gedacht kan ook nog worden aan de uitoefening van bevoegdheden in de controlesfeer, voor zover de toepassing daarvan in de concrete omstandigheden is toegestaan.
[106] Wel kan in de wettelijke regeling van het verkennend onderzoek een grondslag worden gevonden voor het *vastleggen* van informatie uit openbare bronnen omtrent personen die geen verdachte zijn, als ook het vergelijken van die informatie met gegevens uit de politieregisters. Zie Kamerstukken II 1996/97, 25 403, nr. 3, p. 49-50.

het verzamelen van informatie. Derhalve geldt hier hetgeen dat is vastgesteld met betrekking tot de algemene taakstellende bepalingen.

6 Conclusie

Noch in het bestuursrecht noch in het strafrecht bestaat een bevoegdheid die specifiek gericht is op het grote schaal vergaren van informatie op internet. In dit rapport zijn wij nagegaan of en zo ja: onder welke voorwaarden de inzet van webcrawlers binnen de opsporing en handhaving toelaatbaar moeten worden geoordeeld. De centrale vraag was:

> *Onder welke voorwaarden is binnen de handhaving en opsporing het verzamelen van informatie door middel van Web Voyager, meer in het algemeen de inzet van webcrawlers, en het gebruik van die informatie rechtmatig?*

Aan de hand van hetgeen hierboven is uiteengezet komen we tot het volgende. De vraag naar de toelaatbaarheid kan niet in algemene zin worden beantwoord. Er is discussie mogelijk over de vraag of zowel binnen het bestuursrecht en meer in het bijzonder binnen het strafrecht bestaande bevoegdheden toereikend zijn om webcrawlers als Web Voyager in te zetten. Ongeacht of er nieuwe regels nodig zijn voor een (expliciete) bevoegdheid om informatie verkregen door internetcrawlen binnen de opsporing en handhaving te gebruiken, geldt dat voor de inzet van webcrawlers procedurele waarborgen noodzakelijk zijn.

6.1 Bevoegdheid webcrawling en huidige regelgeving

Binnen het bestuursrecht kan informatie over de naleving van wettelijke voorschriften worden verkregen via uitoefening van de bevoegdheden die een toezichthouder op grond van de Awb of de bijzondere wet heeft, maar kan ook op andere wijze verkregen informatie, zoals via webcrawling, in beginsel worden gebruikt bij besluitvorming over oplegging van een bestuurlijke sanctie. Webcrawling is geen toezichtshandeling waarop art. 5:13 Awb (evenredigheidsbeginsel) van toepassing is, maar feitelijk bestuurshandelen waarop onder meer de artikelen 3:2 tot en met 3:4 Awb van toepassing zijn. De eisen aan gebruik bij webcrawling zijn minder streng dan die bij gebruik ervan in het kader van strafrechtelijke opsporing, wat in geval van gebruik van strafrechtelijk onrechtmatig verkregen bewijs binnen de handhaving van betekenis kan zijn.

Bij het opstellen van de bevoegdheden in het Wetboek van Stafvordering en bijzondere wetten kon een technologie als webcrawling niet worden voorzien. Vooralsnog heeft de ontwikkeling van die technologie niet de aandacht van de wetgever genoten. Het onderbrengen van webcrawling bij bestaande bevoegdheden is niet eenvoudig. Algemene taakstellende bepalingen alsmede webcrawling als onderdeel van een verkennend onderzoek bieden een fragiele grondslag, omdat deze niet toereikend zijn indien de resultaten van webcrawling te zeer ingrijpen in de persoonlijke levenssfeer van de betrokkene. In de specifiek wettelijk geregelde opsporingsbevoegdheden kan een grondslag nog het beste worden gevonden in een combinatie van de bevoegdheden tot stelselmatige observatie en stelselmatige inwinning van informatie. Uitgaande van een dergelijke grondslag is de inzet van webcrawlers aan beperkingen onderhevig.

De uitspraak van het Europese Hof van Justitie in 2014 waarin de dataretentierichtlijn ongeldig werd verklaard, biedt interessante aanknopingspunten voor webcrawling. De massaliteit van de verzamelde informatie is vergelijkbaar, waarbij de zorgen over inbreuk op de persoonlijke levenssfeer in versterkte mate gelden bij webcrawling. Belangrijk verschil is dat bij dataretentie uitspraak getoetst werd of op grond van een bestaande wettelijke plicht en een dergelijke expliciete grondslag vooralsnog ontbreekt. Uitgaande van toelaatbaar verzamelen hangt de vraag of webcrawling een inbreuk oplevert van het recht op bescherming van de persoonlijke levenssfeer als bedoeld in art. 8 EVRM af van de aard van de verkregen informatie en of een min of meer compleet beeld ontstaat van bepaalde aspecten van het persoonlijk leven van een persoon. Een belangrijk punt dat uit de uitspraak volgt is dat de opslag op zichzelf, hoe ingrijpend ook, gerechtvaardigd kan zijn, mits er voldoende waarborgen in acht worden genomen.

6.2 Normen en waarborgen bij inzet webcrawlers

6.2.1 Mogelijke normering webcrawlers

In de Awb zouden regels opgenomen kunnen worden over het gebruik van andere instrumenten dan de in titel 5.2 genoemde bevoegdheden. Ongeacht hoe gericht een webcrawler het internet opgestuurd wordt, het is niet goed denkbaar om webcrawling te reguleren op basis van welke inbreuk op de privacy was te verwachten op het moment dat de webcrawler wordt ingezet. Dat maakt het moeilijk en maar wel van belang om in wetgeving *in algemene zin* nauwkeurig te regelen onder welke omstandigheden bepaalde activiteiten die kwalificeren als webcrawling al dan niet toelaatbaar zijn. Het is daarbij vereist dat in de wettelijke regeling wordt bepaald in welke gevallen de bevoegdheid tot webcrawling bestaat, hoe ver de vergaring van informatie mag strekken en welke autoriteit beslist omtrent de inzet van webcrawling. Het is lastig om exact aan te geven welke informatie wel en niet mag worden vergaard. Om die reden zou ervoor kunnen worden gekozen om informatievergaring in ruime mate toe te staan, maar dan wel een strikte normering te kiezen waar het gaat om het bewaren, bewerken en gebruiken van de informatie.

Meer nog dan normering van het verzamelen van informatie, zou normering zich kunnen richten op de wijze waarop vervolgens van de verzamelde informatie gebruik wordt gemaakt. Dit is een ingewikkeld vraagstuk dat zich leent voor nader onderzoek. Vooruitlopend daarop volgen hieronder enkele oriënterende gedachten.

6.2.2 Systeem van controle en rechtsbescherming

Voor het bepalen of informatie verkregen door webcrawlers gebruikt mag worden, speelt een rol in hoeverre is voorzien in een adequaat systeem van controle en rechtsbescherming om misbruik te voorkomen en in het bieden van gelegenheid te reageren op bevindingen. Een noodzakelijke maatregel daarbij is het loggen van webcrawlingactiviteiten: wie heeft, wat, wanneer gedaan.

Via webcrawling verkregen informatie zou in beginsel eerst moet worden voorgelegd aan betrokkene, voordat zij ten grondslag kan worden gelegd aan een ingrijpend bestuursrechtelijk besluit. Voorkomen moet worden dat een burger consequenties van activiteiten van webcrawling ondervindt, zonder de mogelijkheid te worden geboden de resultaten te weerleggen. De neiging is om wat de technologie aandraagt als juist te zien, maar ook als “computer says yes” kan het eigenlijke antwoord nee zijn.

Binnen het strafrecht zal een notificatieverplichting – vanwege de grote schaal waarop informatie wordt ingewonnen – een grote administratieve last kunnen opleveren. Gekozen zou kunnen worden om betrokkenen niet te informeren over via webcrawling verkregen suggesties die nergens toe leiden. Het is dan echter wel noodzaak om op een andere (meer meta)niveau toezicht te organiseren op een juiste omgang met de gegevens. Tot die juiste omgang behoort ook het vernietigen van gegevens wanneer deze geen rol meer spelen in een onderzoek en er ook anderszins geen noodzaak bestaat voor het langer bewaren daarvan.

6.2.3 Organisatorische inbedding data analyse

Binnen de politie houdt de informatieorganisatie zich bezig met:[107]

> “Voorziet de politie van actuele informatie die noodzakelijk is voor de uitvoering en sturing van politiewerk, en creëert overzicht en inzicht in de (inter)nationale en veiligheidssituatie. Dit doen de medewerkers onder meer door het verzamelen van informatie, analyseren en adviseren. De landelijke informatieorganisatie regelt internationale informatie-uitwisseling en coördineert nationale informatie.”

[107] https://www.politie.nl/themas/politietaken.html

Een dergelijk eenheid, al dan niet een subonderdeel ervan, lijkt zich te lenen voor de inzet van webcrawlers. Gezien de kracht van de webcrawling technologie moet voorkomen worden dat een doorsnee agent te pas en te onpas gebruik van een dergelijk systeem zou kunnen maken. Beter is om de bevraging van de verzamelde informatie en de daarop los te laten analyses over te laten aan mensen die gespecialiseerd zijn in data analytics.

Ook zou er voor gekozen kunnen worden om de analytische activiteiten, zoals op dit moment ook bij Webvoyager het geval is, te laten plaatsvinden buiten de reguliere politieorganisatie. Bedrijven als FOX-IT doen op dit moment opsporingswerk, maar leiden tegelijkertijd zowel politie als legermensen op. Het opleiden van mensen die vervolgens binnen de politieorganisatie analytische werkzaamheden kunnen verrichten, lijkt ons te verkiezen boven aan opsporing gerelateerde werkzaamheden door private partijen te laten uitvoeren. Gezien de gevoeligheid van handhavings- en opsporinginformatie is het raadzaam om specialisten onderdeel van de politieorganisatie te laten uitmaken.

6.3 Slotopmerkingen

In dit rapport is ingegaan op de voorwaarden waaronder op internet aanwezige informatie met behulp van webcrawlers verzameld mag worden. Een vervolgvraag is welke bewerkingen er vervolgens met die informatie toelaatbaar moeten worden geacht. Deze vraag leent zich voor nader onderzoek. Het antwoord op die vraag zou er zelfs toe kunnen leiden dat vanwege de waarborgen die ten aanzien van de verwerking in acht worden genomen, het op ruime schaal vergaren van gegevens met behulp van technische middelen geen schending van het recht op de persoonlijke levenssfeer behoeft op te leveren.